National Institute for Intelligence Studies

RISR No. 21/2019

ROMANIAN INTELLIGENCE STUDIES REVIEW

EDITURA ANIMV

"MIHAI VITEAZUL"
NATIONAL INTELLIGENCE ACADEMY

ROMANIAN INTELLIGENCE STUDIES REVIEW

No. 21/2019

The *Romanian Intelligence Studies Review* is an academic journal with scientific prestige, acknowledged by the National Council for the Validation of University Titles, Diplomas and Certificates (CNADTCU), indexed in the international databases CEEOL and EBSCO. For more information please visit the official website www.rrsi.ro.

Bucharest
2019

CONTENT

INTELLIGENCE AND INTELLIGENCE STUDIES IN THE 21ST CENTURY

INTELLIGENCE AND INTELLIGENCE STUDIES. TIME FOR A DIVORCE?

Bob DE GRAAFF*

Abstract

Many in intelligence still follow Sherman Kent's doctrine of intelligence as a type of social science that should try to develop natural science-like laws which make predictions possible. However, his positivist and realist approach is outdated in the academic world. It would be fruitful for both intelligence and intelligence studies to leave Kent's positivist legacy behind. Constructivism offers much more profitable prospects, especially for intelligence studies, whose academic status is endangered by clinging to an outdated positivism. Meanwhile intelligence, which has often used Kent's ideas as an ideology to fend off intelligence consumers, should do better to no longer pretend to come close to a science. Instead, using Aristoteles division in episteme (science), techne (tradecraft) and phronesis (practical wisdom), intelligence analysis should be seen as practical wisdom (phronesis) for practical decision-making. This would allow intelligence to embrace cognitive diversity in order to proffer different kinds of policy support. Leaning toward constructivism would help intelligence to become more action-oriented instead of information-oriented under the doom of positivism. Following the diverging paths of episteme for intelligence studies and phronesis for intelligence analysis, both should play their own autonomous roles, which would still leave meetings between the two useful.

Keywords: *Intelligence analysis – positivism – constructivism – Sherman Kent – phronesis.*

Introduction

The relationship between intelligence and academic studies is not fixed. Firstly, some practitioners of intelligence studies see them as the study *for* intelligence, i.e. being more practically oriented, trying to

* Professor for intelligence and security studies University of Utrecht, email: b.g.j.graaff@uu.nl.

train students for a career in intelligence, whereas others favour intelligence studies to be studies *on* intelligence, i.e. more reflexive and meant not only to educate future intelligence practitioners, but also future diplomats, journalists, employees of NGOs and so on. Secondly, both inside and outside the intelligence communities there is debate whether intelligence analysis is an art or something close to science (e.g. Herbert, 2013, 653).

Collaboration and exchange of thoughts between (former) practitioners of intelligence and those who study intelligence can be fruitful, just as they can be between military and practitioners of war studies or between diplomats and students of international relations. My argument is that it would nevertheless be good for both intelligence and intelligence studies if the two could become disentangled, leaving no doubt about the own roles of the respective practitioners.

In this contribution I will try to demonstrate how some propagate ideas about intelligence as if it is (almost) a science that can hardly be distinguished from the study that should take it as its object, and show that these ideas have taken the form of an ideology for some, whereas presenting intelligence as a (near-)science may actually hamper positive results and become a burden for the practice of both intelligence and intelligence studies. By pretending that intelligence it should be some kind of science the former is hampered in fulfilling its proper role of proffering guidance to decision-makers in an uncertain world and the latter is thwarted in achieving a better academic status than its current one.

In order to appreciate this argument one will have to take into account differences between the US and Europe, especially regarding the divergent educational systems.

Commonalities and differences between intelligence analysts and academics

At first sight intelligence analysts and academics have much in common. They may have been taught at the same universities or colleges. Because analysts can be academically trained they are sometimes known as the 'eggheads' of the intelligence community. Sherman Kent wrote already in 1949: 'intelligence organizations must

be not a little like a large university faculty. […] They must guarantee a sort of academic freedom of inquiry and they must fight off those who derogate such freedom […]' (Kent 1971, 74). Admiral Stansfield Turner, head of the CIA under President Jimmy Carter, boasted that his service 'had more Ph.Ds. than any other area of government and more than many colleges' (Turner 1986, 113; cf. Smith 1976, 59).

To what extent can intelligence analysts and academic scholars be compared? The work of analysts resembles in many respects that of scientific researchers. They formulate hypotheses, operationalize key concepts, are concerned about presuppositions, analyse data, interpret and integrate those, distinguish between major and minor issues, draw conclusions and try to present their findings as clearly as possible. Many of the methodical recommendations for intelligence analysis are therefore reminiscent of the Research Methodology classes at a university.

Nevertheless, there are some important differences between intelligence analysts and scientific researchers. The pressure of time to come up with an analysis is much greater for intelligence organizations than for research at universities. This may have consequences for the validity of the outcomes. Furthermore consumption of the intelligence products is often limited to brief reports. Scientists mainly work for the long term, while the product of intelligence analysts is usually geared to the short term. It also worth noting that scientific research rarely involves deliberate deception by its research object, while an intelligence analyst must take elusive behaviour by target this into account. In addition, scientists can test their provisional findings at (international) symposia and conferences or in papers before they record their final findings. Because of the secret nature of their work, intelligence analysts often cannot. On the other hand, analysts may have access to secret information that is (temporarily) unavailable to scientific researchers.

Although both professional groups use hypotheses, their functions differ. Scientists start their research with hypotheses which they use to verify or falsify them in whole or in part, while intelligence analysts start their research with targets and then build data-based hypotheses of which the degree of probability is indicated. Finally,

intelligence analysts write to concrete consumers who have formulated their needs for practical knowledge, while scientists often do not know who can and wants to benefit from their (sometimes theoretical) knowledge.

As Agrell and Treverton stated in their 2015 book *National Intelligence and Science*: science and intelligence constitute indeed 'two remarkably similar and interlinked domains of knowledge production, yet ones that are separated by a deep political, cultural, and epistemological divide' (Agrell and Treverton 2015, 3). It is this epistemological divide that will be addressed in this contribution, a divide that seems to have grown over time.

Kent's ongoing legacy

One of the first books on modern intelligence systems considered the founding text of modern intelligence was *Strategic intelligence for American World Policy* (1949) written by Sherman Kent, who during the Second World War had worked for the CIA-predecessor Office of Strategic Services (OSS), specifically its Research and Analysis Branch, 'perhaps the most ambitious effort to merge academia and intelligence in the analysis phase of the intelligence process during World War II' (Agrell and Treverton 2015, 19). After a brief period back at his alma mater Yale University Kent returned to the intelligence world in 1950, where he came to be regarded as 'the father of modern intelligence analysis', with his ideas influencing 'not just the United States but also its friends and allies as well' (Agrell and Treverton 2015, 48).

Kent was a historian by training. Just when he entered the world of intelligence in 1941 he was about to publish *Writing History*, of which it was said that if you replaced the word 'historian' by 'intelligence officer' you would have a good guide for intelligence analysis (Ford 1980, 2). Kent had certain ideas about how intelligence analysis should look like, which he not only presented in his aforementioned book about strategic intelligence, but also especially in two articles, which are still often cited: one about the need for an intelligence literature and the other about words of estimative probability (Kent 1955, 1964). According to Kent, in 1955, the intelligence profession had 'taken on the

aspects of a discipline: it has developed a recognized methodology; it has developed a vocabulary; it has developed a body of theory and doctrine; it has elaborate and refined techniques.' The only thing that was still lacking then was a literature by intelligence's 'most knowledgeable devotees', its 'master practitioners', 'practicing members of the profession' especially about techniques and methods, some kind of house organ literature plus (Kent 1955), a defect that has since been remedied: *Studies in Intelligence*, the CIA in-house publication about techniques and methods, which Kent helped to establish. In short, Kent developed intelligence into a science of analysis, characterized by a strict methodology (cf. Kreuter 2010, 252, 261-262), which in its turn should lead to 'nothing less than a science of prediction', a hubric and elusive aspiration. (Scoblic 2018).

Today Kent's ideas still have a great influence on the self-image of many who work in intelligence. More than three decades after his death his name still figures foremost in the indices of intelligence textbooks and it is sometimes amazing to see how little has changed in the general ideas many have of intelligence analysis over more than half a century since the writings of Kent. Kent's ideas about intelligence analysis have not only become 'the foundational theory of intelligence', they seem to be 'an unquestionable intelligence orthodoxy' (Woodard 2013, 91).

Kent's ideas were anchored in his time and therefore his legacy in intelligence became 'the ongoing legacy of positivism' (Kreuter 2015, 218). These ideas could be summarized as follows (for an elaborate presentation with numerous examples see: Kreuter 2010 and Lillbacka 2013). The mission of intelligence is to see the development of threats earlier than its masters. The masterpiece of intelligence analysis estimates. Intelligence analysis comes closest to social science. Because the task of intelligence is to be prognostic, it would be nice if there would be something like social science laws akin to natural science laws, based mainly on causation and inferences. In order to develop such laws rigorous methods are needed. Or, as Sherman Kent wrote in 1949:

> 'Truth is to be approached, if not attained, through research guided by a systematic method. In the social sciences which

> largely constitute the subject matter of strategic intelligence, there is such a method. It is much like the method of physical sciences. It is not the same method but it is a method none the less. […] In spite of […] great disadvantages, social scientists go on striving for improvements in their method which will afford the exactness of physics or chemistry' (Kent 1971, 156).

The premise for such a science-oriented intelligence analysis was that reality exists independently of people's observations and interpretations. Cognitive limitations can be overcome, e.g. by reducing biases. Propositions can be adjudicated by systematic methods. Propositions or models correctly describing reality are true. Language is a neutral medium for communicating 'reality'. Communication itself is neutral. Accurate descriptions of reality allow for predictions.

In the positivistic or realistic tradition in which Kent stood it is acknowledged that people's interpretations of the world may be faulty, but these faults may be corrected by using a right set of methods, which, mainly thanks to Richards Heuer, came to be known in the intelligence world as structured analytic techniques, and by critical thinking. By clarity of wordings it would be possible to transfer ideas to consumers of intelligence, often policy- or decision-makers. However, the latter are not to be influenced, as the intelligence producers and their products are claimed to be objective, non-partisan and neutral (cf. Woodard 2013, 99). In order to maintain this objectivity and neutrality on the part of the intelligence analysts there should be a virtual wall between the producers and the consumers of intelligence. Or as Nathan Woodard aptly articulates it by analogy to the Bible book Genesis: 'In the beginning there was Sherman Kent. And Kent said: "thou shalt not be policy prescriptive in thine intelligence"' (Woodard 2013, 91-92). And ever since when intelligence producers and intelligence consumers come too close to each other there are 'cries of corruption and scandal' (Lammana 2011, 1).

Against this idiosyncratic backdrop the intelligence producers claim to speak truth to power, avoiding that their products become the victim of politicization, i.e. 'the compromise of the objectivity of intelligence, or of how intelligence is used, to serve policy or political aims.' (Pillar 2012, 473)

It is neither possible nor necessary to run the whole gamut of expressions of dominantly positivistic ideas in the intelligence world. Suffice to show a few illustrations, such as in the early years of the CIA when Allen Dulles in 1947 pleaded for an agency 'whose duty is to weigh facts, and to draw conclusions from those facts (…) The Central Intelligence Agency should have nothing to do with policy'' (quoted in Lamanna, 2011, 54-55) and when Admiral Roscoe H. Hillenkoetter, head of the CIA, stated in 1948, a year after the creation of the agency, that the task of an intelligence analyst consisted of 'endlessly putting fact upon fact, until the whole outline appears', thus 'providing the factual basis for high-level policy decisions affecting our national security' (Hilsman, 1952, 3). Such attitudes are still prevalent seventy years later, as shown e.g. by the exhortation by former Director of National Intelligence James Clapper: '"tell it like it is" – straight, objective, unpoliticized' (Clapper 2018, 358, 398).

As said, it is astounding to see how little the so-called scientific outlook of the intelligence community has changed over the years. As Wilhelm Agrell noted:

> 'The conduct of intelligence in terms of technological basis, collection ability and focus changed dramatically during the twentieth century. What did *not* change in a corresponding way was the underlying theory of cognition, the idea that in the end intelligence is about facts, about the "real" world, and that this will be revealed more or less by itself through a linear and to an increasing extent industrialized knowledge-production system. […] There has been only limited and scattered development of the field [of intelligence analysis] since the publication of Sherman Kent's classical book on strategic intelligence in 1949' (Agrell 2012, 129-130).

And actually this is how Kent had intended it to be. For an historian he had a remarkable belief in the permanency of ideas. In a 1966 preface for a reprint of his 1949-book he wrote that, in spite of an augmentation of the intelligence community's task, the principles he had set forth in 1949 would 'always be with us': 'whatever the new

wrinkles, the eternal verities remain': 'the thoughtful effort of bright and studious people conducting their business within the very broad limits of the scientific method is the thing which did the trick', the sum of a great many facts and a method of combining them, and not 'a few rules of the thumb, an appeal to folk wisdom, and a little intuition' (Kent 1971, xviii, 48 and xxi-xxii). After Kent the intelligence shop for science was closed. Kent resembled a defector who told his new masters that every defector who would come after him would be a false one.

Agrell in 2015, this time joined by Greg Treverton, commented on the lack of scientific progress in the intelligence world:

> 'Why did half a century of debate over the importance of a scientific dimension in intelligence analysis lead to such remarkably meagre results? Why has a field so rapidly developing and of such high priority as intelligence not transformed long ago in this direction as a continuation of professionalizing? What we thus should look for is perhaps not the incentives for a science of intelligence to develop but rather the reasons it failed to do so' (Agrell and Treverton 2015, 23).

And the first and foremost reason Agrell and Treverton give for the missing incentives is that intelligence producers keep their tradecraft secret in order 'to draw a sharp dividing line between insiders and outsiders, those in the know and those not in the know and thus by definition unable to add something of substance'. Academic penetration was seen as just as bad as or even worse than hostile penetration (Agrell and Treverton 2015, 24-25).

While Dulles's and Hillenkoetter's statements in the late 1940s could still be seen in line with general ideas in science, which at the time was dominated by empiricism, positivism, realism and optimism about the possibility of developing natural science-like laws in the social sciences, seen from the perspective of today's science many of the elements in the above outlook seem terribly out of date. Facts, threats, truths, communication and language are no longer seen as realities in and of themselves but as constructions.

Science as ideology

Former intelligence analyst Nathan Kreuter characterizes the U.S. intelligence community's adherence to positivism and the concomitant idea of neutral language as an ideology (Kreuter 2015). An ideology is a collection of normative beliefs and values that an individual or group holds for other than purely epistemic reasons. It claims to offer the key interpretation of a certain reality and the ultimate solution to its defects. In the world of intelligence it is mostly political ideologies that are known, such as fascism, communism, nationalism and populism. However professional groups can have ideologies as well, such as medical personnel, social workers or academics. And although '[s]tudying ideologies is not the same as producing them' (Freeden 2003, 71), the cluster of above-mentioned positivistic ideas such as the neutrality and objectivity of intelligence analysis and the need for a wall between intelligence producers and consumers can take on the cloak of an ideology as well. After all, 'the claim of an "apolitical" status is itself a very political claim' (Kreuter 2010, 45).

The best type of ideology is the one that is not detected, that presents itself as neutral, as self-evident normalcy and thus has such a persuasive force that it does not lead to questioning. Such an ideology is the self-concept of intelligence, which presents itself as a-political knowledge or science shielded from the same politics it is supposed to serve, 'a protective mechanism to prevent decision makers from politicizing finished intelligence' (Marrin 2007, 409). However, in order to seem self-evident an ideology needs to have a certain footing in reality.

This does not mean that ideology and practice overlap. Thomas L. Hughes, Assistant Secretary of State for Intelligence and Research under the Presidents Kennedy and Johnson, maintained that in spite of the philosophy of the wall between intelligence and policy the American practice has been characterized by 'intelligence in search of some policy to influence and policy in search of some intelligence for support' (Maurer, Tunstall and Keagle 1985, 11). Others too have aired the opinion that the reigning practice in intelligence analysis is intuition, not science or scientific methodology, not even the use of structured analytic

techniques, for which there is often too little time due to the pressure to produce timely and actionable intelligence (Dahl 2012; Khalsa 2009; Marrin 2011, 42-44; Coulthart 2016, 942; Chang et al. 2018).

An ideology can excel by shielding itself off from possible criticism by giving its guardians an authoritarian esoteric status, which makes it nigh impossible for outsiders to contest its preconceptions. Except for religious groups, where could this be done better than in secret organizations, where 'intelligence seeks to secure for itself the authority of expertise' (Kreuter 2010, 35)? There is another link with religion in the sense that the positivistic ideology makes itself untouchable, as testified by descriptions of the so-called wall between intelligence producers and consumers as 'the "sacred curtain"', 'the catechism of the intelligence officer' or his 'basic ethic'(Schmitt 2005, 53; Heyman 1985, 57; Stansfield Turner quoted in Lamanna 2011, 95)

Ideally ideologies are meant to either support aspirations to a certain position or, once these positions have been reached, defending a status quo. Once the ideology has been accepted as the dominant paradigm it can prevent challenges to its core ideas. In that respect the Kentian positivism has been remarkably successful. Although there is a wealth of incitements to new theoretical underpinnings and approaches of intelligence (e.g. Bean 2018), the Kentian approach and the structured analytic techniques are still the dominant doctrine. A remarkable number of intelligence failures has not led to lasting criticism of this dominant approach. On the contrary, since 9/11 the view that intelligence should be seen as a scientific enterprise has increased and this time even the U.S. National Research Council pleaded for such an approach (Agrell and Treverton 2015, 86-87; Dahl 2012; Committee 2011). The ironic outcome of the 2001 and the Iraq-weapons of mass destruction intelligence failures is that in the end they favoured structured analytic techniques, because they have the advantage that they leave behind an audit trail (Agrell and Treverton 2015, 86). These so-called SATs have even been mandated by the Intelligence Reform and Terrorism Prevention Act of 2004 and have been codified in U.S. Intelligence Community Directive 203. And with the introduction of big data and artificial intelligence the naive

factualism and the idea that data are neutral and not context-bound and as such facilitate predictions may even further prolong the positivist approach in intelligence. (Lillbacka 2013, 318; Scoblic 2018).

Enter constructivism

While intelligence still clings to positivism, following Kent's hope that the social sciences may one day more or less mirror the natural sciences, most social scientists today acknowledge that the overambitious imitation of the natural sciences has created a crisis in the social sciences. They now recognize that if science is supposed to deliver untouchable knowledge then there is little science in it. For instance in complexity sciences, there is a 'realization that we have reached the cultural end of certainties', that it is chaos and complexity that rule the world today, that crisis is permanent (Wallerstein, 2004, 38; Cavelty & Mauer, 2009, 136). Or in postmodern sciences it is accepted that today we are confronted with 'multiple, overlapping and often contradictory narratives' (Cavelty & Mauer, 2009, 134). In the words of the American sociologist Immanuel Wallerstein: we will have to live "with the knowledge that uncertainty […] seems to be the only intractable reality" (Wallerstein, 2004, 56).

Just as positivism was fashionable in science in 1949, when Kent wrote his catechism for intelligence analysis, so is constructivism today. Constructivism does not view reality as objective and given but departs from the idea that the interaction of human minds (re)creates reality. Constructivism offers the most coherent exposure of the shortcomings of the Kentian positivistic/realistic approach in intelligence. While realism may still have worked at a time that intelligence was mainly 'evaluation and comparison of military strength based exclusively on numerical factors', also known as bean-counting, (Agrell 1983, 184-185; cf. Colby 2007; Kivett 2006, 44), constructivism fits much better in a world where intelligence is pre-occupied with intentions and with complexities or wicked problems, which are hard to define, ever-changing, never at rest and which can only be solved by re-defining them through a different discourse or narrative. Constructivism is also better in explaining information and influence operations as part of at least some major intelligence organizations in the world. If accepted as

the leading philosophy behind intelligence instead of Kentianism, constructivism would have tremendous effects not only for the practice of intelligence but also for the way it is studied. What constructivism is or aspires to be can best be shown by juxtaposing it to Kent's positivism and realism (cf. Rathbun 2007).

Tabel 1: Positivism and constructivism approaches (author's perspective)

	Positivism/realism	**Constructivism**
Perception	Objectively real	Intersubjective
Nature of reality	Objectively real	Socially constructed and malleable but often reified as objectively real
Problems of uncertainty	Lack of information	Ambiguity of information
Conception of uncertainty	Ignorance (epistemic or aleatory)	Indeterminacy of a largely socially constructed world that lacks meaning without norms and identities
Challenge of uncertainty	Judge intentions of others	Ascribe meaning
Tools for reducing uncertainty	Information	Norms and identities
Learning	Addition of information for better representation of reality ('updating')	Acquisition of identities and interests through socialization and persuasion leading to normative change
Bias	Error to be eradicated	A given
Language	Neutral and self-evident provided clarity	A rhetorical means to (re)create the world

Communication with consumers	Disseminating a product (finished intelligence)	An ongoing process of joint sense- or meaning-making
Responsibility of intelligence	Ends with dissemination of a good intelligence product	Includes good decision(s) based on good intelligence
Predictions	Possible thanks to accurate descriptions of the objective reality	= performative means to shape reality
Rationality	Instrumental rationality (*Zweckrationalität*)	Value rationality (*Wertrationalität*)
Course of consumers	Act upon (actionable) intelligence	Persuade and influence in order to cause normative change/ (re)creating and (re)defining reality/ strategic communication and construction
Power	Based on intelligence (information advantage leads to decision advantage)	Performativity (the power of language to effect change)
Relations with other entities	Antagonistic (intelligence success of one is the failure of other; no friendly services)	Depending on the performative act : antagonistic or inclusive

How different the two approaches are may become clear from the way the concept of 'common sense' would function in both approaches. To realists common sense means accepting reality as it is. Everything that deviates from that viewpoint is nonsense. To constructivists nothing in the world seems 'common' or 'normal'. In principle there are endless possibilities of defining and redefining the world. Common sense would mean to constructivists that a collective

of individuals or entities shares the same outlook. If one has to indicate an overriding principal difference between the two stances it is that positivist/realist Kentians associate intelligence with the realm of information and constructivists associate intelligence with the realm of persuasion (cf. Woodard 2013, 95). It typifies two ways of thinking about intelligence as Wilmoore Kendall had already noticed in 1949. Kent, said Kendall, did not look upon the course of things as 'something you try to influence but as a tape all printed up inside a machine; and the job of intelligence is to tell the planners how it reads.'(Kendall 1949, 549).

Therefore, although constructivists pay a lot of attention to language, e.g. in the way of text or discourse analysis, the application of constructivism in the world of intelligence would make intelligence much more action-oriented than it is under the current dominant doctrine, which leaves action as a responsibility to the consumer (cf. Rahbun 2007, 552). Such an action-oriented view of intelligence is much more in sync with current developments that stress intelligence's role in influencing behaviour, information operations and strategic communication.

Farewell to positivism in intelligence studies

For certain reasons (i.e. its secretive nature) knowledge about the practice of intelligence has for a long time depended upon the insights of (former) practitioners. A quick overview of intelligence textbooks shows that many of its authors have had experience in the intelligence community. However, the greater the transparency of government, the easier it becomes for outsiders to study government activity. This is also true for the field of intelligence studies. When there was little public knowledge about state's intelligence activities, the insider's knowledge was of great importance. Over the past half century, however, more and more has become known about intelligence activity, to such an extent that it is not difficult to drown in the libraries that have been filled with intelligence monographs and textbooks as well as on the Internet (cf. Scott & Jackson 2004, 139-140; cg the bibliographies on www.iafie-europe.org).

The influence former intelligence practitioners hold over intelligence studies can also be explained by institutional arrangements in U.S. academia, which, in spite of recent developments in Europe, is still the world's major hub of intelligence studies. In the U.S. educational system it is possible to enter academia at an advanced age after a long career in intelligence. Therefore it is not uncommon that intelligence studies are taught by former practitioners. This has guaranteed that the teaching about intelligence has stayed close to the practice of a field where inside knowledge used to be hard to gain. It also meant that the main tendency in intelligence studies was the study *for* intelligence. At the same time it condemned intelligence studies to a relatively low academic status as the list of academic merits of some of these U.S. professors of intelligence studies was rather short.

In Europe it has often been the other way around. It took much longer to get intelligence studies established as an academic discipline. At the same time only those who have finished a Ph.D. get a tenured position at universities and the list of academic merits before one becomes a full professor has to be very long. Because those teaching academic intelligence studies in Europe follow the same tracks as their academic colleagues their academic status is relatively high. Late entries from other career paths almost impossible. Intelligence studies are thus mostly taught by people with little or no direct experience in the intelligence world. The intelligence studies that are taught in Europe are often studies *on* intelligence.

In spite of their more elevated status teachers and students of intelligence at European universities run the risk of jeopardizing their position in academia when they stick to the outdated positivistic knowledge that is often recorded in intelligence textbooks. If these academics who often have to operate within international relations departments or in the field of security studies do not demonstrate the idea that security is a contested concept and that men construct their realities they run the risk of becoming the laughing-stock of their departments. Furthermore, as Scott and Jackson wrote already in 2004: 'An uncritical acceptance of official or semi-official representations of the intelligence process as singularly free of ideological assumptions and political biases leaves the intelligence

scholar open to the familiar charge that she or he is merely legitimising and perpetuating the ideology of the state'(Scott and Jackson 2004, 12). All this hampers the integration of intelligence studies into broader disciplines such as international relations studies (Petersen & Rønn 2019, 315; Scott & Jackson 2004). Let alone that taking the government's perspective makes it difficult to develop *critical* intelligence studies, which would demonstrate how particular narratives become privileged or devalued in the intelligence production process (Kreuter 2010, 43-44).

It is therefore time to 'decolonize' intelligence studies from its referent object, which has manifested itself as its referent subject for too long now. Literary authors do not dictate what is taught in literature studies, diplomats not what is taught in international relations studies and deceased people not what is taught in history classes. Why should it be different in intelligence studies, if it wants to be taken seriously as an academic discipline?

Farewell to the claim for science in intelligence

Meanwhile, should intelligence cling to the outdated so-called scientific approach, while intelligence studies to part from it? The risk of the intelligence world sticking to the currently dominant approach is that it leads to overconfidence in representing the reality where this should not be the case. The scientist Kentian approach has stood in the way of maturing the intelligence process itself. To mention just one example, the idea of a wall between intelligence producers and consumers has, in spite of the idea that intelligence has a support function for decision-makers, led to amazingly little interest in the receptivity of decision-makers for information and the relation between knowledge or information on the one hand and decisions on the other (cf. Woodard 2013, 101).

The wall-argument is an impediment for thinking about the question how information can be disseminated with a maximum or optimal impact, other than some generalities, e.g. about the form in which knowledge should be distributed. Major questions whether information of and by itself has an impact or that emotions should be involved to create impact are side-lined. Previous mind-sets or decisions

of intelligence consumers are hardly taken into account apart from the cliché that today decision-makers have access to more and more information channels of their own. Established beliefs on the part of the intelligence consumers that stand in the way of accepting intelligence analysis seem in intelligence studies to be almost the sole preserve of dictatorships like the Soviet Union and Nazi Germany, not of that of leaders of the free Western World. The general idea is still that after receiving the facts the decision-maker will be convinced and will make the correct decision, and if he does not, it his fault or her stupidity.

Let us see what would happen if one would accept that the positivistic approach of intelligence is something that should not only be left behind by intelligence studies, but also by the intelligence world itself. In that case there are two options. The first is to impose more advanced scientific methods on the intelligence communities. The second option is for the intelligence communities to say goodbye to the ideological scientist claims.

The first road is recommended by e.g. David Mandel and Philip Tetlock:

> 'The IC needs a diverse infusion of ideas from scientists outside the IC. It needs those scientists not only to put forward their best ideas, but also to test them in rigorous experiments or experimental tournaments. The IC should take the most promising results and work with scientific teams to transition these ideas into analytic processes' (Mandel and Tetlock 2018, 4).

It will be clear that in my opinion this is likely to be a dead-end road that will only prolong the shortcomings that followed from the optimistic scientist approach that was begun by Sherman Kent. The second option, to say goodbye to the scientist claims, was ironically given by Richards Heuer in August 2010, when it was suggested to him to have his method of analysis of competing hypotheses, the so-called ACH-method, the crown jewel of the SATs, tested empirically. His reaction was:

> 'Can't we have confidence in making a *common sense judgment* that going through the process of assessing the inconsistency of evidence will generally improve the quality of analysis? Similarly can't we have confidence in making a *common sense judgment* that starting the analysis with a set of hypotheses will, on average, lead to better analysis than starting by looking at the pros and cons for a single hypothesis? (…) If the empirical testing of my two claims about the value of ACH doesn't replicate exactly how ACH is (or should be used in the Intel Community, I would be inclined to ignore it and stick with my *common sense judgment*.'(Quoted in Mandel and Tetlock 2018, 3; italics by me).

Here we come to the kernel of the issue. Forced to choose between the intelligence community's pseudo-science and real science, Heuer gave three cheers for common sense judgments. However, there is no need to be triumphant about Richards Heuer's late confession, because I think the most important thing to note here is that Heuer recognized the real function of intelligence: to reduce the government's ignorance, as David Omand calls it in three ways: by building situational awareness, deliver explanations for the behaviour and motivation of other actors, and prediction (Omand 2010, 24-25).

The rigidity of using certain methods often does not help to realize these goals. The emphasis on methods may lead to the neglect of material expertise (Mandel and Tetlock 2018, 4). Intelligence expert Greg Treverton drew this lesson from experience: 'The more we required our analysts to be explicit about their methods, the more we risked turning them into middle-weights' (Treverton 2007, xviii). After all, there are a lot of analytic issues that would require very little scientific analysis; rather keeping a score-card or filling a matrix would suffice (cf. Herbert 2013, 655-657). As Herbert stressed: it is much better for intelligence analysts to use problem-solving techniques that draw promiscuously from multiple sources of intellectual virtue and professional specialization and 'to embrace cognitive diversity than to seek out a theoretical unity that serves no practical purpose […] While "science" sounds good as part of a catch phrase, its methodological nuts

and bolts have little applicability to intelligence analysis.' (Herbert 2013, 663), where the diversity of issues at stake requires quite diverse types of analysis support (Herbert 2013, 659-660).

Consequently, the practical knowledge that is required does not have to be science. As Greg Treverton writes, since 'truth' cannot be known in a 'blizzard' of uncertainty and complexities, intelligence's standard is and should be 'good enough for government work' (Treverton, 2009, 54), which fits in with Elbridge Colby's conclusion: 'When training the new generation of analysts, therefore, the intelligence community should focus not on achieving the hopeless twentieth-century dream of taming human life through predictive social science, but rather on the murkier but more realistic categories of practical wisdom and intuition'(Colby 2007). Such practical knowledge for (practical) decision-making is also known as phronesis in Aristoteles' epistemology.

Three types of knowledge

Aristoteles' epistemology distinguishes between three types of knowledge: episteme (theoretical know why), techne (tradecraft based upon experience) and phronesis (practical knowledge in support of practical action in a certain context). Or we could say: science, technical tradecraft and phronesis. If one understands intelligence analysis as 'actionable knowledge' or rather actionable foreknowledge (Rønn & Høffding 2013, 709, 711) or, as Sherman Kent stated in his *Strategic Intelligence*, 'knowledge […] which is capable of serving as a basis for action' (Kent 1971, 5), it can be categorized as phronesis according to Aristoteles' division and distinguished from episteme or science. Intelligence reports then come close to what in earlier times was the mirror for princes, also known as *specula principum* or *Fürstenspiegel*, such as for instance Sun Tzu's *On War*, Kautilya's *Arthashastra* from ancient India or Machiavelli's *The Prince* (cf. Lamanna 2011, 5). Such phronesis concerns the analysis of things that are good or bad for men as a point of departure for action (Flyvbjerg, 2006, pp. 4, 57). The central questions of such phronesis are: 1. Where are we going? 2. Is this desirable? 3. What should be done? 4. Who gains and who loses? (Flyvbjerg, 2006, 60, 130-131). Such questions end in shaping reality

rather than describing it. They fit in well with the value- and action-orientation of constructivism, while saving an information-orientation. They are also the type of questions that can be answered both by intelligence and intelligence studies, but both from their own relatively autonomous position.

I do not wish to say that intelligence (analysts) and academia should not cooperate. On the contrary, recognition of the separate roles which intelligence collectors and analysts on the one hand and academics on the other play makes both strategic alliances and ad hoc meetings between the two all the more necessary. However, such cooperation should be done while recognizing that intelligence analysts represent phronesis and academics represent episteme or science, two types of knowledge which should not be confused. At the same time both analysts and academics would do well to recognize that realities as such do not exist but that it is images and narratives of reality that matter and that those are the results of power positions. Such a recognition fits in better with action-oriented constructivism than with the so-called reality-oriented positivism. Time for both the intelligence world and intelligence studies to say goodbye to the latter.

References:

1. Agrell, Wilhelm, (1983). 'Beyond Cloak and Dagger', in: Wilhelm Agrell and Bo Huldt (ed.), *Clio Goes Spying. Eight Essays on the History of Intelligence*, Lund: Lund Studies in International History 17.
2. Agrell, Wilhelm, (2012). 'The Next 100 Years? Reflections on the Future of Intelligence', *Intelligence and National Security*, 27, 1, 118-132.
3. Agrell, Wilhelm and Gregory F. Treverton (2015). *National Intelligence and Science. Beyond the Great Divide in Analysis and Policy*, Oxford etc.: Oxford University Press.
4. Bean, Hamilton, (2018). 'Intelligence theory from the margins: questions ignored and debates not had', *Intelligence and National Security*, 33, 4, 527-540.
5. Bracken, Paul, (2006), 'Net Assessment: A Practical Guide', *Parameters*, Spring, 90-100.

6. Cavelty, Mary Dunn & Victor Mauer, (2009). 'Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence', *Security Dialogue*, 40(2), 123-144.
7. Chang, Welton et al., (2018). 'Restructuring structured analytic techniques in intelligence', *Intelligence and National Security*, 33, 3, 337-356.
8. Clapper, James R., (2018). *Facts and Fears. Hard truths from a life in intelligence*, New York: Viking.
9. Colby, Elbridge, (2007), 'Making Intelligence Smart', Hoover Institution Policy Review no. 144.
10. Committee on Behavioral and Social Science Research to Improve Intelligence Analysis for National Security, National Research Council (2011). *Intelligence Analysis for Tomorrow. Advances from the Behavioral and Social Sciences*, Washington D.C.: National Academies Press.
11. Coulthart, Stephen, (2016). 'Why do analysts use structured analytic techniques? An in-depth study of an American intelligence agency', *Intelligence and National Security*, 33, 7, 933-948.
12. Dahl, Erik J., (2012), 'Pinball Wizards and Professors: Competing Models of Intelligence Analysis', paper prepared for presentation at the International Studies Association annual conference, San Diego, California, April.
13. Davis, Jack (1991). 'The Kent-Kendall Debate of 1949', *Studies in Intelligence*, vol. 35, 2, 37-50.
14. Flyvbjerg, Bent, (2006). *Making Social Science Matter. Why social inquiry fails and how it can succeed again*. Cambridge: Cambridge University Press.
15. Folker, Robert D., (2000). *Intelligence analysis in theater joint intelligence centers: an experiment in applying structured methods*, Washington D.C.: Joint Military Intelligence College.
16. Ford, Hal P., (1980). 'A Tribute to Sherman Kent', *Studies in Intelligence*, 24, 3, 1-8.
17. Freeden, Michael (2003). *Ideology. A Very Short Introduction*, Oxford etc.: Oxford University Press.
18. George, Alexander L., (1969). 'The "Operational Code": A Neglected Approach to the Study of Political Leaders and Decision-Making', *International Studies Quarterly*, 13, 2, 190-222.
19. Herbert, Matthew, (2006). 'The Intelligence Analyst as Epistemologist', *International Journal of Intelligence and Counterintelligence*, 19, 4, 666-684.

20. Herbert, Matthew, (2013). 'The Motley of Intelligence Analysis: Getting over the Idea of a Professional Model', *International Journal of Intelligence and Counterintelligence*, 26, 4, 652-665.
21. Heyman, Hans, (1985), 'Intelligence Policy Relationships', in: Alfred C. Maurer, Marion D. Turnstall and James M. Keagle (ed.), *Intelligence. Policy and Process*, Boulder, CO/London: Westview Press, 1985, 57-66.
22. Hilsman, Roger, (1952). 'Intelligence and Policy-making in Foreign Affairs', *World Politics*, 5, 1, 1-45.
23. Kendall, Willmoore, (1949). 'The Function of Intelligence', *World Politics*, 4, 1, 542-552.
24. Kent, Sherman, (1971). *Strategic Intelligence for American World Policy*, Princeton, NJ: Princeton University Press, (1949).
25. Kent, Sherman, (1955). 'The Need for an Intelligence Literature', *Studies in Intelligence*, September, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sherman-kent-and-the-board-of-national-estimates-collected-essays/2need.html.
26. Kent, Sherman, (1964). 'Words of Estimative Probability', *Studies in Intelligence*, vol. 8, 4, 49-65.
27. Khalsa, Sundri, (2009). 'The Intelligence Community Debate over Intuition versus Structured Technique: Implications for Improving Intelligence Warning and Analysis', *Journal of Conflict Studies*, 29.
28. Kivett Esq., Philip G., (2006). *Intelligence Failures and Decent Intervals*, Bloomington, IN/Milton Keynes: Author-House.
29. Kreuter, Nathan Allen, (2010). Rhetorical Intelligence: The Role of Rhetoric in the US Intelligence Community (Ph.D. Thesis University of Texas at Austin).
30. Kreuter, Nathan Allen, (2015). 'The US Intelligence Community's Mathematical Ideology of Technical Communication', *Technical Communication Quarterly*, 24, 217-234.
31. Lamanna, Lawrence J., (2011). Theoretical reasons for variations in the intelligence-policymaking distance in the United States and the United Kingdom (Ph.D. Theses University of Georgia).
32. Lillbacka, Ralf G.V., (2013). 'Realism, Constructivism, and Intelligence Analysis', *International Journal of Intelligence and Counterintelligence*, 26, 2, 304-331.
33. Mandel, David & Philip E. Tetlock, (2018). 'Correcting Judgment Correctives in National Security Intelligence', *Frontiers in Psychology*, 9, December, 1-5.

34. Marrin, Stephen, (2007). 'At arm's length or at the elbow? Explaining the distance between analysts and decision makers', *International Journal of Intelligence and Counterintelligence*, 20, 3, 401-414.
35. Marrin, Stephen, (2011). *Improving Intelligence Analysis. Bridging the gap between scholarship and practice*, London/New York: Routledge.
36. Maurer, Alfred C., Marion D. Turnstall and James M. Keagle (ed.) (1985). *Intelligence. Policy and Process*, Boulder, CO/London: Westview Press.
37. Medina, Carmen A., (2002). 'The coming revolution in intelligence analysis. What to Do When Traditional Models Fail?', *Studies in Intelligence*, 46, 3, 23-29.
38. Mitzen, Jennifer & Randall L. Schweller, (2011). 'Knowing the Unknown Unknowns: Misplaced Certainty and the Onset of War', *Security Studies*, 20, 1, 2-35.
39. Nolan, Bridget, (2018). 'Ethnographic Research in the U.S. Intelligence Community: Opportunities and Challenges', *Secrecy and Society*, 2, 1, https://scholarworks.sjsu.edu/secrecyandsociety/vol2/iss1/5.
40. Olcott, Anthony, (2009). 'Revisiting The Legacy: Sherman Kent, Willmoore Kendall, and George Pettee - Strategic Intelligence in the Digital Age', *Studies in Intelligence*, 53, 2, 21-32.
41. Omand, David, (2010). *Securing the State*, New York: Columbia University Press.
42. Ormerod, Owen (2018). Advancing the epistemology of intelligence analysis: a Polonyian perspective (master thesis Deakin University).
43. Petersen, Karen Lund & Kira Vrist Rønn, (2019). 'Introducing the special issue: bringing in the public. Intelligence on the frontier between state and civil society', *Intelligence and National Security*, 34, 3, 311-316.
44. Petersen, Karen Lund & Vibeke Schou Tjalve, (2018). 'Intelligence expertise in the age of information sharing: public-private "collection" and its challenges to democratic control and accountability', *Intelligence and National Security*, 33, 1, 21-35.
45. Pettee, George S., (1946). *The Future of American Secret Intelligence*, Washington D.C.: Infantry Journal Press.
46. Pillar, Paul, (2012). 'The Perils of Politicization', in Loch K. Johnson (ed.) *The Oxford Handbook of National Security Intelligence*, Oxford, New York: Oxford University Press, 472-484.
47. Rathbun, Brian C., (2007). 'Uncertain about Uncertainty: Understanding the Multiple Meanings of a Crucial Concept in International Relations Theory', *International Studies Quarterly*, 51, 533-557.

48. Rønn, Kira Vrist & Simon Høffding, (2013). 'The Epistemic Status of Intelligence: An Epistemological Contribution to the Understanding of Intelligence', *Intelligence and National Security*, 28, 5, 694-716.
49. Schmitt, Gary J., (2005) 'Truth to Power? Rethinking Intelligence Analysis', in: Peter Berkowitz (ed.), *The Future of American Intelligence*, Stanford, CA: Hoover Institution Press, 41-64.
50. Scoblic, J. Peter, (2018). 'Beacon and Warning: Sherman Kent, Scientific Hubris, and the CIA's Office of National Estimates', *Texas National Security Review*, 1, 4 (August), http://doi.org/10.15781/T2J38M448.
51. Scott, Len and Peter Jackson, (2004). 'Journeys in Shadows', in: idem (ed.), *Understanding Intelligence in the Twenty-First Century. Journeys in Shadows*, London/New York: Routledge, 1-28.
52. Scott, Len and Peter Jackson, (2004). 'The Study of Intelligence in Theory and Practice', *Intelligence and National Security*, 19, 2, 139-169.
53. Sharot, Tali, (2017). *The Influential Mind. What the brain reveals about our power to change others*, London: Abacus.
54. Smith, Joseph B., (1976). *Portrait of a Cold Warrior*, New York: Putnam.
55. Tang, Jeffrey, (2017). 'How do we know? What intelligence analysis can learn from the sociology of science', *Intelligence and National Security*, 32, 5, 663-674.
56. Treverton, Gregory F., (2007). 'Commentary', in: David T. Moore, *Critical Thinking and Intelligence Analysis*, Washington D.C.: National Defense Intelligence College, xvii-xviii.
57. Treverton, Gregory F., (2010). 'Addressing "complexities" in homeland security', in: Loch K. Johnson (ed.), *The Oxford Handbook of National Security Intelligence*, Oxford etc.: Oxford University Press, 343-358.
58. Treverton, Gregory F., (1994). 'Estimating Beyond the Cold War', *Defense Intelligence Journal*, 3, 2, 5-20.
59. Treverton, Gregory F., (2009). *Intelligence for an Age of Terror*, Cambridge etc.: Cambridge University Press.
60. Turner, Stansfield, (1986). *Secrecy and Democracy. The CIA in Transition*, London: Sidgwick and Jackson.
61. Wallerstein, I., (2004). *The Uncertainties of Knowledge*. Philadelphia: Temple University Press.
62. Warner, Michael, (2012). 'Intelligence and Reflexivity: An Invitation to a Dialogue', *Intelligence and National Security*, 27, 2 (2012), 167-171.
63. Woodard, Nathan, (2013). 'Tasting the Forbidden Fruit: Unlocking the Potential of Positive Polticization', *Intelligence and National Security*, 28, 1, 91-108.

INTEGRATING INTELLIGENCE PRACTICE AND SCHOLARSHIP: THE CASE OF GENERAL INTELLIGENCE AND SECURITY SERVICE OF THE NETHERLANDS (AIVD)

Ingmar WESTERMAN*

Abstract

This text is a revised version of the keynote speech that the author delivered at the 2019 conference of the European chapter of IAFIE. The conference took place in Bucharest and was hosted by the Romanian National Intelligence Academy "Mihai Viteazul". A considerable number of European intelligence and security services participated in this gathering of intelligence practitioners and scholars dedicated to intelligence education. The text makes a case for integrating intelligence practice and scholarship, drawing attention to some of its conditions, reasons and benefits. Several examples ranging from established AIVD routine to some of the service's latest initiatives stress the significance of a close(r) cooperation between intelligence work, its study and other academic disciplines and perspectives.

Keywords*: intelligence education; integrating intelligence scholarship and practice; IAFIE; AIVD*.

Introduction

Intelligence and scholarship may seem like two different worlds. The world of intelligence, traditionally closed, specialized in knowing and keeping secrets, having exclusive sources and privileged access to well-positioned decision makers. On the other hand the academic world, open by nature, transparent about its sources, with reproducible methods and falsifiable results, working from the assumption that knowledge needs to be shared to grow.

* Dr. Ingmar Westerman is a practitioner in the field of countering extremism, email: ingmar.westerman@minbzk.nl.

The point I like to make is that these two worlds can and in certain cases and circumstances should not just be connected but even integrated. In order to do so, intelligence and scholarship should be viewed not as two different worlds but as two domains of "knowledge production" that can and, under certain conditions, should be combined (Agrell & Treverton, 2015). I will give a few instances of how AIVD integrates scholarship and academic perspectives with its daily work. Then I will sketch several elements that form the background or context of why such integration is needed. These elements are 1) the nature of some of the main threats against national and international security, 2) the limited, and I suspect decreasing capabilities of states to entirely control or manage such threats, and 3) the question of legitimacy in both academic and intelligence domains.

I will conclude with a few suggestions on what these reflections mean for intelligence education. These are 1) teach and stimulate intelligence officers, not just analysts, to activate their academic (you may also call it reflective or critical) potential, also outside of their intelligence routine, 2) train and enable them, again not just analysts, to apply their newly acquired knowledge and reflective skills within their work, make them learn to ask new questions, and use new sources or use old sources differently, and 3) incorporate and institutionalise academic researchers and research within the intelligence community.

But first let me clarify what I mean with scholarship. The scholars I refer to are not just those working within the discipline of 'intelligence studies', with academic knowledge of the history, cultures, dealings and methodologies of intelligence work. With scholars I mean all those professional academics, from a variety of disciplines and sub disciplines (whether sociology, psychology, international relations, political theory, anthropology, criminology, theology, as well as those academics specialised in extremism, terrorism, technology, public administration and those focusing on certain countries and regions) that can help to understand and to interpret events and trends, people and phenomena that may affect national and international security.

When I talk of integrating intelligence practice with scholarship I must address a possible objection first. There are scholars and surely others who mistrust the objectivity of government institutions,

especially the secretive arm of the state. Quite a lot has been written and said about the undesirable steering of independent scholarship as part of the securitisation of society at large. Where I say integration, some see co-optation and compromise. My plea for integration is about equal partnership, not for meddling or manipulation. To those who remain unconvinced I can say that independence is as much a core value of intelligence and security services in a democratic society as it is for universities and other centres of learning. Practitioners are well aware of the sensitivity and intrusive character of their work and that is an important reason why they should cherish their own objectivity and autonomy but equally those of others. The AIVD motto is a Latin phrase which translates as 'against the current'. As long as both domains cling to their own independence independently, I think they can safely be integrated.

What is inevitable for a more inclusive model is that both domains lose some of their exclusivity. Scholars have to admit that academic contributions can and will be made by others who are not always formally or fulltime part of academia. Just as hard, or maybe even harder, practitioners will have to accept that some of their work can be enhanced and critically assessed by scholars who are not part of their intelligence community. This may well be another objection, and a double-edged one, against being too hopeful about integration. On the other hand, it can also be seen as a sign that in this case integration would not lead to assimilation in which one side would be absorbed into the other, having to conform completely. Leaving these and other objections aside, I proceed to emphasise the benefits.

Scholarship and intelligence practice are different domains, not necessarily different worlds. These domains can profit from each other and (on certain topics relating to national and international security, and on the condition of mutual independence) can reinforce each other mutually when working much more closely together than is usually the case. Scholarship has a lot to teach practitioners, like conceptual clarity, methodological complexity and parsimony, and critical reflection. Intelligence practice, on the other hand, has lots of unique data and the possibility of acquiring even better data, the means to mix open source information with closed sources to produce better informed and more

accurate assessments, and privileged access to the higher reaches of politics. It is the integration of these domains for which I like to make a case.

Instances of integration

Let me give you a few examples. The first instance is a report we published 15 years ago, and which we, and others still draw on today. The second one is a very recent partnership that we started with Delft University of Technology in the field of national cyber security. The third example discusses the final instance which is the joint panel organised by Leiden University, the Academy "Mihai Viteazul" and AIVD on connecting intelligence theory to analytical practice.

In 2005, AIVD published *From dawa to jihad* (the Dutch version was published the year before). It was an unclassified report aimed at the general public. You can find it on our website and other spaces on the internet. It is a text which, certainly then, was not considered a typical intelligence product. It is among other things a conceptual exercise, defining the specifics of Islamic radicalisation and its connections to jihad. It also elaborates the notion of democratic legal order, both as a form of government and a kind of society (AIVD, 2005). Its definition of dawa (the propagation of radical Islam) even made it into the Dutch dictionary. The report is based on the interpretation and generalisation of the intelligence that our service assembled in its investigations into jihadism and radical Islam, as well as on academic consultation and on literature from several disciplines like sociology, political theory and religious studies. We and others still draw on the main findings of that report and the report that followed (AIVD, 2007). I mention those unclassified reports written for a wider audience as early examples of integrating intelligence practice and scholarship. Several European agencies now write public reports with a comparable mix of intelligence and scholarship. A very recent example is the theme report on the background of right-extremists in Norway by PST, the Norwegian security service (PST, 2019).

Since several months Delft University of Technology and AIVD cooperate closely on national cyber security. A full professor of that university, an expert on the intersection of technological innovation and

public administration, has recently joined our ranks part-time, together with a colleague with the same background from Leiden University. They bring with them five researchers (both PhD and postdoc). The programme will run for a five year period. Some of the topics to be researched and published on involve data-driven innovations, machine learning, the complexity of cooperation on national cyber security, and private or citizen intelligence. In order to come up with new and relevant conclusions they join as part-time colleagues, and will have access to anonymised (big) data. One of the side effects of incorporating scholars may be that other colleagues get actively involved academically, and can be triggered to lecture, publish, or perhaps start their own PhD research. By incorporating scholars and activating colleagues in such a way, many new questions arise. How to select and prepare data? What kind of data can be declassified or kept unclassified? Do such data yield different results than publically available data? Most of those questions trigger responses and new practices that will further enhance the integration of scholarship and intelligence practice.

The AIVD archive has a modest reputation for academic, mainly historical disclosure. Two authorised histories of the BVD, AIVD's forerunner, were written by a former colleague as an in-house historian who had access to considerable parts of the archive. The first of those books was also his doctoral dissertation (Engelen, 1995). The last one deals with the cold war period and dates from 2007 (Engelen, 2007). Since then several studies were undertaken, always with restricted access for academic outsiders (Wiebes, 2015, Hijzen, 2016). We have very recently decided to put our archive's hidden treasures to even better use, as well as the expertise and experience of some our colleagues. A selection of historians among them, with either a master's or a doctor's degree, are specifically tasked. For a limited amount of their time they will look at the archive from an historian's point of view, to determine which events, episodes and epochs deserve special attention, and may be prepared for further research and publication. To do this well, these colleagues need to be or get up-to-date with relevant literature and stay or get into contact with professional scholars. This is what I call the activation of academic potential. One of the advantages, I

hope, is that this may pave the way for integrating outside scholars, a sensitive issue, to do justice to the historical value of our archive without of course compromising sources or secrets or those of partner services.

A fourth and final example is the conference's panel on how to tailor analytical approaches to real-world intelligence problems, which AIVD organised jointly with the Academy "Mihai Viteazul" and Leiden University. The topic was chosen to stress the importance of bringing academic theory and intelligence practice to bear on each other. We opted for a panel organised collectively to underline the need to approach this particular topic together, combining the efforts of an intelligence academy, a university and a security and intelligence service. Under the title 'How to analyse what?' we address several methodological challenges such as complexity and the integration of diversity into teaching intelligence practitioners. Seeing the number of participants at this conference on mapping the future of intelligence education, among which so many partner services, and given the recent founding of Intelligence College in Europe (ICE, 2019), I am convinced that the cooperation between the domains of scholarship and intelligence practice will still grow closer.

Need for integration

Why is the integration of intelligence work with scholarship important? A short answer from the perspective of an intelligence- and security service such as AIVD is that it helps us to safeguard national security. A more mutual answer, which includes a more academic point of view, is that without it will be hard to understand and interpret the threats and challenges that face all of us. I like to add some layers of context or background. Three of those layers are the nature of the threats, the diminishing capacity of governments to control or manage them adequately and finally the question of legitimacy. The significance of integrating intelligence practice and scholarship depends on all three.

In the first place, the nature of today's threats demand joint efforts. What threats like terrorism, extremism, espionage, foreign state interference, cyber threats and others have in common is that they defy easy categorisation and require all the help we can find. National security is not something that can be secured by intelligence- and

security services just by themselves, not even when we cooperate as closely as we do. Take the well-known but poorly understood threat of ultra-orthodox Islam known as Salafism. What is it exactly? When and why is it a threat? What makes it different from other ultra-orthodox belief systems? And so on. Or look at the manipulation of information and information technology. When exactly is it a threat to national security? How to separate foreign and domestic threats? These are questions for which intelligence and security services need a hand. Or two.

Most of today's and tomorrow's threats and challenges to (inter)national security are too complex, too multi-layered and too unmanageable to be handled in the old fashioned way, by seemingly omnipotent governments. That holds true for many issues, but certainly matters of national security are especially important as far as the diminishing capacity of any government working in a democratic way is concerned. Control and certainty are in short supply nowadays. One of the possible effects is democratic regression, the rise of a certain kind of politics that promises simple solutions and complete control. This situation affects the legitimacy of governments and their intelligence and security agencies negatively. At the same time, the authority and the legitimacy of independent scholarship is also put under stress. Both domains have a common interest in maintaining their authority and independence. For these interconnected reasons the integration of scholarship with intelligence work, on specific topics and under certain conditions, is significant.

The third layer is that of diminishing legitimacy. Of states, but along with it, also of intelligence services. At least since Edward Snowden they confront an increased political, legal and public demand for compliance, oversight, and, if that is the right word, transparency. Pierre Rosanvallon's term 'legibility' is perhaps more appropriate, since it is tied to acute democratic requirements (Rosanvallon, 2018). In times of endless availability of information and organised distrust, secrecy is no longer always an advantage. A much closer connection with the academic domain may be part of the answer. By joining forces what may be called a crisis of legitimacy can be confronted. Both domains face similar challenges in a time in which fact and fiction are easily confused and manipulated, and in which nonsense and ill-

founded fears of conspiracies are cultivated. The trustworthiness and authority of both academics and intelligence practitioners (as well as other categories such as journalists) is questioned. Working more closely together on matters of national security may help both domains to maintain their own integrity and independence.

Benefits for intelligence education

What does a tight connection between intelligence practice and scholarship mean for the future of intelligence education? Please allow me to approach this from an agency-centric point of view. I distinguish three steps which are mutually reinforcing but also have a logical and chronological order: 1) teach and stimulate intelligence officers, certainly not all of them but not just the analysts, to use their academic reflective and critical skills and contacts to *activate* academic potential from within the agency; 2) train and enable them to *apply* and perhaps *adapt* academic concepts, conclusions, doubts and criticisms and so embed them deep within the intelligence process, and 3) *incorporate* scholars and academic institutions within the intelligence community. These steps, and you can see that they are formulated from the point of view of an agency, may sound intrusive and will sometimes be hard to realise. Intelligence education may help to ease the way.

Firstly, how to academically activate a part of the intelligence workforce? Let me be clear, I am not making the case for turning many intelligence officers into professional academics. But I suggest more can be done with the academic backgrounds, interests, skills and connections than is now often the case. But what holds these people and their organisations back? A main reason is that working with(in) intelligence can be, and often is, restrictive business. From the first day on the job you are immersed in a totally new environment in which confidentiality and compartmentalisation are the standard. You get taught how to devise a cover story, and are given many reasons why not to talk about what kind of work you do. You learn how to turn the conversation to other subjects than those that interest you professionally. All with good reason. But there are equally good reasons to also teach how to engage actively in a public, academic setting.

One way of doing that is by educating intelligence officers throughout their careers to invest in learning and networking. Intelligence officers can be taught how to contribute to academic research, to teach, maybe supervise students, encourage some to publish, maybe do doctoral research and write a dissertation, educate them how to balance the conflicting demands of having access to sensitive sources, information and *modus operandi* and being confident about contributing publicly to discussions on matters that concern national security.

After activating the academic potential you need to apply what you have learned deep within your organisation. Put differently, you have to internalise it organisationally. How can intelligence education help to accomplish this? You should train your staff to match practice with theory. Let me give a few examples. For instance, a fairly recent topic in terrorism studies and in criminology is the so-called crime-terrorism nexus. There is a lot of theorising on how criminal and terrorist pathways intersect. How to test and apply these insights and theories? By applying them, I suggest, to data to which intelligence officers have privileged access, maybe by adding them to their own hypotheses. Do we see criminal and terrorist trajectories intersect? Do our 'targets' make more sense with one of several theories in mind? Or, reversely, can certain theories be improved on the basis of our data and analysis?

Let me give an example from a different academic discipline. If you truly want to understand how autocrats, elected or not, behave and position themselves in their our own countries or geopolitically, you must eavesdrop and know what they are plotting, but equally important is the logic of autocratic politics about which you can find plenty in the literature. Intelligence officers are extremely well placed to apply and test such insights and theories, or maybe even enhance these insights and theories by having learned from applying them consciously and carefully. The application of academic knowledge and methodology is something that can and, I think, should be part of intelligence curriculum.

The third and final phase, to incorporate scholars and academic institutions within the intelligence community needs little explanation. Representatives of two domains in which critical thinking is endorsed, many disciplines merge and an endless array of perspectives are

considered and reconsidered will easily find themes and topics to address jointly. Eventually, the presence of professional academics within intelligence communities is itself an incentive for even more scholarly activation and application as they become part of what you may call an educational intelligence cycle. This may well lead to an increase of intelligence practitioners in academic roles and functions. With their mutual incorporation intelligence practice and scholarship become truly integrated.

References:

1. Agrell, Wilhelm & Treverton, Gregory, (2015). *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*. Oxford: Oxford University Press.

2. AIVD, (2005). *From Dawa to Jihad: The Various Threats from Radical Islam to the Democratic Legal Order*, on https://english.aivd.nl/publications/publications/2005/03/30/from-dawa-to-jihad.

3. AIVD, (2007). *The Radical Dawa in Transition: The Rise of Islamic Neoradicalism in the Netherlands*, on https://english.aivd.nl/publications/publications/2007/10/09/the-radical-dawa-in-transition.

4. Engelen, Dick, (1995). *De Geschiedenis van de Binnenlandse Veiligheidsdienst*. Den Haag: Sdu.

5. Engelen, Dick, (2007). *Frontdienst: De BVD in de Koude Oorlog*. Amsterdam: Boom.

6. Hijzen, Constant, (2016). *Vijandbeelden: De Veiligheidsdiensten en de Democratie, 1912-1992*. Amsterdam: Boom.

7. ICE, (2019). Intelligence College in Europe / Collège du Renseignement en Europe, on https://www.intelligence-college-europe.org

8. PST, (2019). *What is the background of right-wing extremists in Norway?* On https://www.pst.no/globalassets/artikler/utgivelser/theme-report_-what-is-the-background-of-rightwing-extremists-in-norway.pdf.

9. Rosanvallon, Pierre, (2018). *Good government: Democracy beyond Elections*. Cambridge, MA: Harvard University Press.

10. Wiebes, Cees, (2016). "Operatie Leunstoel: BVD/CIA-afluisteroperaties in Sovjet- en Oostblokambassades". *Samen met de CIA: Operaties achter het IJzeren Gordijn*. Amsterdam: Boom.

TRANSFORMATIVE LEARNING FOR INTELLIGENCE AND INTELLIGENCE STUDIES

Ms. Julie Mendosa*
Dr. Dennis Westbrooks*

Motto: *"Transformative learning processes result in significant and irreversible changes in the way a person experiences, conceptualizes and interacts with the world"*
Chad Hoggan, Ed.D

Abstract

Intelligence professionals work in a global environment that is complex and rapidly-changing. Intelligence analysis calls for individuals and organizations to adapt their thinking to emerging situations that may challenge existing mental frameworks. Changes to mental frameworks are considered transformations within transformative learning theories. Transformations occur when an individual person's beliefs, values and assumptions that filter incoming information undergo a shift or expansion (Mezirow, 1997). This paper applies the concepts of transformative learning theories to the development of intelligence professionals. The paper proposes that transformative learning among intelligence analysts is important for the performance of analysis and explores how organizations can intentionally foster transformative learning and development.

Keywords: *transformative learning, transformation, adult learning, intelligence analyst, development*.

*Director of Undergraduate Studies, National Intelligence University, USA, email: julie.mendosa@dodiis.mil.
*Director of Continuing and Professional Studies, National Intelligence University, USA, email: dennis.westbrooks3@dodiis.mil.

Introduction

The security environment of the 21st Century is composed of rapidly-changing threats that challenge the mental models of United States intelligence professionals and put national security at risk. Furthermore, technology is advancing faster than humans' ability to understand and manage the new capabilities (Danzig et al., 2018). This complicates an analyst's ability to anticipate what today events mean is, and what tomorrow's events might be. Making sense of all this requires adaptations in the way intelligence analysts think. Transformative learning theories may be able to make important contributions to intelligence analysis. Intelligence organizations that encourage transformational learning will enhance their development of analysts who can shift their mental approaches with changing situations. The theoretical framework of this paper is derived from complementary approaches found in the work of Jack Mezirow (1997, 2000) and Robert Kegan (2000). Mezirow's transformation theory addresses adult learning and development, with attention to ways mental frameworks can become more encompassing of divergent ideas and experiences. Kegan's constructive developmental theory looks at developmental changes to individuals' meaning-making structures.

The paper begins with the paradigm-shifting world in which intelligence work occurs. Relationships between people and within issues are ever-changing, calling for flexible analytic capabilities. The second section describes transformational learning theories, proposed here as a lens for considering analyst's adaptive growth. It begins with the foundational theory of Jack Mezirow and continues with Robert Kegan's constructive developmental approach to learning (Drago-Severson, 2004; Kegan, 2000). The third section explores transformative learning at the National Intelligence University. The final section offers suggestions for intelligence organizations to foster transformational development. Let's begin with a window into the challenges facing intelligence analysts and their organizations.

Intelligence Work Requires Adaptive Thinking

Human thinking is astoundingly capable, but we can be caught unprepared to grasp the meanings of dynamic conditions around us. Ongoing development is essential for analysts to keep up with the changing paradigms that drive global, regional, and local conditions. Human thinking has natural tendencies that shape our meaning-making and decisions (Heuer, 1999; Kahneman, 2011; Lowenthal, 2017). Intelligence scholars have pointed out the ways these tendencies limit objectivity, clarity, and criticality. But they can be stretched; humans grow and develop throughout the lifespan (Drago-Severson, 2004). Transformative learning opportunities can enhance analysts' abilities to be adaptive, critical thinkers. This paper offers transformative learning theory as a lens for considering analyst development. The following few paragraphs introduce the global and human context in which this proposal is made.

The World Is Complex

Intelligence analysis exists in a complex setting: human society. Conditions in which people live, and decisions they make, can change rapidly. Truth can be more relative than fixed in many situations. James Cockayne (2016) introduces new mental models in his global look at interactions between governance, power, and crime. He provides examples of the increasingly crossed paths between these topics from the past twenty years. Issues cannot easily be categorized as political or criminal, though people addressing them have been inclined to sort them in those ways. Cockayne points out how criminal groups with ties to other types of networks such as governance and licit business can shape their own strategic environments. Power and influence in the international arena seem to have become more difficult to understand. The book conveys a new mental model for thinking about transnational organized crime. It demonstrates the ongoing need for anyone addressing these interrelated issues of crime, governance, and power to adapt his or her thinking to see them in new ways. Cockayne's message is appropriate for intelligence professionals, whose work can touch on issues such as governance and transnational crime, as well as many others that are equally complex.

Intelligence Organizations and Analysts Need to Adapt

Josh Kerbel (2004) wrote about the tendency of intelligence professionals to expect human and organizational systems to behave in linear ways. The significant problem with this tendency is that human systems are too complex to be understood by linear thinking. Kerbel explains that components of a human system have ongoing interactions with each other, shaping new behaviours in non-linear ways. He believes intelligence addressing non-linear issues requires broad, big-picture perspectives, and mental processes using synthesis more than analysis (because analysis means to break something into parts).

Intelligence professionals can benefit from a capacity to reassess assumptions and shift perspectives. Mark Lowenthal (2017), a noted intelligence scholar, indicates objectivity and critical thinking are essential abilities for analysts. One common pitfall in analysis, identified by Lowenthal, is the tendency to expect others to behave as one's own self or culture would (mirror-imaging.) Another is failing to look closely at a phenomenon because of expecting it to act like other past events. Lowenthal explains that new types of situations can call for new ways of analysing. A relevant advantage of transformative development, as Mezirow (2000) explains, is that it stretches learners toward an ability to see an event through more than one mental model or perspective. Another is that it helps learners see that they have underlying assumptions, identify the origins of these beliefs, and assess their validity for today's situations. These abilities would be beneficial for critical and objective thinking.

Amy Zegart (2007) opined about the Intelligence Community's failures in adapting to changing terrorist threats prior to the 9/11 attacks. She stressed the importance of recognizing problems of bureaucratic organizations, which are guided by rational self-interest to not take on major reforms that were in the nation's best interests, but not the best interests of individual agencies. The autonomous thinking capacity Mezirow (2000) described in the following section offers a valuable way of understanding development toward adaptive, independent, and responsible thinking (Mezirow, 1997) that can encompass big-picture issues.

Shifting Perspectives through Transformation

Jack Mezirow is the primary foundational scholar of theory regarding perspective transformation (Hoggan, 2016). Mezirow (2000) referred to his own theory as transformation theory; other related approaches from varying scholarly disciplines spring from Mezirow's original work and are part of what Hoggan (2016) calls the metatheory of transformative learning. Hoggan defines transformative learning as "processes that result in significant and irreversible changes in the way a person experiences, conceptualizes, and interacts with the world" (p. 71). This paper will describe Mezirow's theorizing, as well as one of the other related approaches that also falls under the metatheory of transformative learning. The related approach is constructive developmental theory, largely based on the work of Robert Kegan (Drago-Severson, 2004; Kegan, 2000).

Mezirow's perspective transformation theory proposes that each adult has built a framework of beliefs, principles, biases and assumptions of how the world works, based on what the individuals' experiences have meant to him or her. This framework filters and shapes the meanings of the individual's incoming information and experiences (Mezirow, 1997). Ongoing or new experiences can challenge or contradict mental frameworks, causing what Mezirow called a disorienting dilemma (Hoggan, 2016, p. 61). A disorienting dilemma is a situation that does not make sense according to existing mental frameworks. An individual may pause to consider his or her expectations and the assumptions or beliefs that support them (Hoggan, 2016). This reflection has an important role in transformation (Mezirow, 1997). Reflection is triggered through engagement with new ideas or ways of seeing something; Mezirow characterizes this process as discourse.

Discourse is an important way that an individual can become aware of his or her own and others' interpretations and assumptions. Mezirow defines discourse as dialogue meant to help its participants assess an argument and its underlying point of view. Encounters with others' perspectives can trigger self-reflection, leading to awareness of one's own assumptions (Mezirow, 1997). Participants in discourse are exposed to the elements of others' arguments and can assess the

reasons supporting the beliefs in those arguments. This is part of a critical thinking process (Mezirow, 2000). Ultimately discourse enables its' participants to form their own understanding. A new understanding of an experience expands the mental framework, allowing the creation of more encompassing frameworks (Drago-Severson, 2004). According to Mezirow (1997, 2000), a transformation is when the framework changes or expands. Transformations tend to make frameworks more encompassing of divergent ideas and experiences. Mezirow further theorizes that transformations in thinking and learning enable individuals to become autonomous thinkers, reliant on their own values and meanings rather than on authorities or traditions. Kegan (2000) expresses transformational growth as coming to see where one's ideas come from and to think critically about them. In this author's words, an individual can gain the ability to step back from a framework, see it, consider its origins, and determine whether or how it can be applied. This ability is invaluable in intelligence and national security work, as analysts determine what might be going on in the world and what it means.

Transformative learning scholars distinguish between transformational and informational learning (Drago-Severson, 2004). Drago-Severson writes that informational learning is taking in new knowledge and skills, deepening resources within an existing way of knowing. Transformative learning is "a shift in how a person constructs reality" and how he or she makes sense of experience (p. 19). This paper argues that the difference between transformational and informational learning is important in the education of intelligence analysts. Informational learning is essential for analysts. However, the thinking needed for paradigm-changing threats requires analysts to critically question their assumptions. Deepening existing mental frameworks is not enough. The complexity of many issues calls for analysts to understand information in new ways. Intelligence professionals should have opportunities to transform their learning and thinking.

Three Ways of Knowing

Transformations in learning are changes to the ways a person knows or learns (Kegan, 2000). An individual's way of knowing can also

be called an epistemology (Drago-Severson, 2004; Kegan). Transformations in epistemology represent development that takes thinking from concrete forms to more abstract ways of knowing. This is quite different than learning that simply adds knowledge or changes behaviours, such as informational learning mentioned above (Drago-Severson, Kegan). Kegan argues that adults need both knowledge and abstract thinking to be successful in life. This is most certainly true for intelligence professionals.

Drago-Severson (2004) explains that transformational learning theories are based on a premise that learning and growth are lifelong, growth is often gradual, and it trends toward greater complexity. New experiences are processed according to the existing meaning-making system, causing it to gradually shift. The small changes accumulate into larger, more complex mental organizations.

A constructive developmental approach to transformational learning is one of several ways to consider adult development. This approach looks at developmental changes to individuals' meaning-making structures (Kegan, 2000). Kegan identifies three primary ways of knowing that are common for adults and represent developmental levels. Each person might use multiple ways of knowing but is likely to have one that is primary. Kegan's three ways of knowing are instrumental, socialized, and self-authoring. The instrumental way of knowing is the most concrete, and self-authoring is the most abstract.

The Instrumental Way of Knowing

Drago-Severson (2004) summarizes Kegan's adult ways of knowing. Instrumental knowing is concrete, rule-based; knowledge is accumulated and comes from authorities. Differences of opinion mean one is right and another is wrong. The instrumental knower does not hold multiple perspectives at the same time. Decisions are based on following steps or rules, and knowledge is seen as instrumental for achieving goals (Drago-Severson).

The authors expect the instrumental way of knowing in intelligence analysis to favour existing principles (when they are from valid sources) that are commonly applied to the issue. The methodical and verification aspect of structured methods might seem more

important than hypothesis generation. Analysis favouring an instrumental way of knowing might be prone to anchoring, to using a belief system that has worked before, and to making pragmatic decisions that would compromise exploration. This approach could also favour a definition of expertise that is rooted in accumulated information rather than flexible or adaptive understanding. Government organizations can be rule-based, authority-driven, compartmented and specialized. Developing or holding a perspective that is conceptually different from the mainstream can be difficult. The institutional setting itself might make instrumental knowing a likely default in many situations.

The Socialized Way of Knowing

The socialized way of knowing, also described by Drago-Severson (2004), is tied to the beliefs and expectations of others in the social setting. She explains that socialized knowers are better able to sympathize than instrumental knowers and look to others as part of their decision process. Kegan (2000) and Drago-Severson's descriptions indicate that thinking has moved beyond the more absolute, rule-bound approach of instrumental knowing, and can be abstract, generalized, and reflective. Socialized knowers make decisions based on what others expect of them, or what will look good according to social norms for their environment. Drago-Severson indicates conflict or disagreement is a threat to socialized knowers. In intelligence work, this could mean groupthink, following a party line, and being more conscious of existing standards in a field than creative new ways of understanding an issue.

The Self-Authoring Way of Knowing

The self-authoring knower relies on internalized values rather than external, authority-based sources of meaning. The self-authoring knower can integrate or co-exist with competing value systems, can step outside of him or her-self to look at ideas or relationships, and can see knowledge as context-dependent. Conflict, or differences between people, is natural parts of dialogue (Drago-Severson, 2004). Intelligence professionals who are self-authoring knowers might be able to assess the

assumptions underlying ideas or analysis. They might be readily able to consider alternative hypotheses and imagine various potentialities for future events. These are abilities needed for sound analysis according to the ODNI's analytic standards (Intelligence Community Directive 203). Richards Heuer (1999) explained the limitations of mental models that serve as lenses for analysis; the self-authoring knower appears able to consider the presence of a model for the self or others and step out of it or to consider elements of other models.

Adults can gradually shift from one primary level to another over time (Drago-Severson, 2004; Mezirow, 1997, 2000) as they continue to develop. Kegan (2000) expressed that individuals can pass from a condition in which their experience is essentially interpreted for them by principles in the social environment (when they are instrumental and socialized knowers), to an existence they author for themselves (the self-authoring way of knowing). Over time the ability to see frameworks can become the way a person learns, a way of knowing (Drago-Severson, 2004). The literature places these three ways of knowing in a developmental order that begins with instrumental, progresses to socialized, and can develop toward self-authoring. This paper suggests intelligence analysts can benefit by moving from concrete thinking (instrumental) toward more abstract ways of knowing (self-authoring), while still recognizing the importance of building relevant and timely concrete knowledge.

Ongoing Analyst Development

Adults' ability to shift and grow from one way of knowing toward another has implications for intelligence analysts and intelligence organizations. Transformations can move analysts toward increasingly sophisticated ways of knowing and help them imagine new ways to understand issues. We propose that developmental conditions can be created in which analyst growth is likely to occur. Intelligence work environments that support reflection and discourse have an edge over those that do not.

Individual analysts or intelligence managers who move toward more autonomous ways of knowing could be expected to increase their abilities to consider alternative hypotheses, see a situation through

someone else's eyes, and be more interested in collaboration. The US intelligence community's analytic tradecraft standards (Intelligence Community Directive 203) call for analysts to understand their own thinking processes and support their conclusions; these are strengths of self-authoring learners. Transformative opportunities enhance analysts' capacity to understand their own beliefs, and to see those of others. The following section explains some of the conditions that encourage ongoing development in the undergraduate program at the National Intelligence University.

Transformative Learning at the National Intelligence University

The National Intelligence University (NIU) is a federally-administered US educational institution offering bachelor's and master's degrees to mid-career intelligence professionals. NIU is admittedly in a more advantageous position to enhance learning than most work settings, and follows multiple practices that encourage transformative learning. The students are arranged in cohorts, taking numerous courses together. Courses offer content that contains new ideas and perspectives for the students' consideration, and many courses are based on discussion. This format gives students opportunity to engage in discourse with each other, while considering new ways of looking at an issue. They interact with the course content, apply ideas to their work experiences, and reflect individually and as a group on the meanings. These growth-enhancing practices can reasonably be applied to many workday intelligence environments, particularly where analysts are arranged in groups or teams. The upcoming section provides examples of learning that has occurred at NIU. The final section of this paper offers suggestions for creating developmental opportunities in day-to-day work settings.

The National Intelligence University offers students new perspectives on the world. Students are asked to reflect on the practice of intelligence as a profession, consider a wide range of theories, and share in discourse. Marrin (2011) characterized intelligence studies in higher education as "an academic experiment in progress" (p. 89). NIU programs are built with a goal of encouraging autonomous and

responsible thinking as students engage in national security activities. At the end of the academic year, the undergraduate students complete a Capstone project, and graduate students complete a thesis, informed by their coursework and directly tied to their concentration of study. The National Intelligence University prepares the classified Capstone project for the Intelligence Community to add to the body of knowledge on national intelligence priorities, and understanding of security issues.

Mezirow's (1997) guidance to educators is extremely relevant to NIU. The academic year begins with an expectation that each student (adult) prior to his or her arrival at the University, has built a framework of beliefs, principles, biases, and assumptions of how the world works, based on what the individuals' experiences have meant to him or her. In an academic setting like NIU, Mezirow's theory works in unison with Kegan's (2000) constructive developmental approach to learning. As mentioned earlier in the paper, Kegan's approach offers three ways of knowing: instrumental; socialized; and self-authoring. Kegan's three ways of learning can be found among the adult learners in the intelligence community and at NIU. Each learner has a primary way of knowing, but is likely to tap into other ways of knowing when stretched by participating in a cohort of other learners (Drago-Severson, 2004). NIU's undergraduate program supports each of the three ways of knowing, yet simultaneously offers support to students toward development into more abstract thinking.

Instrumental knowing is oftentimes described as tangible, prescriptive, authoritative, and rule-based. All the descriptions are elements found within the Intelligence Community. NIU uses the core curriculum to establish a foundation that embraces instrumental learning. This provides a starting point for understanding United States policy, strategy, capabilities and limitations, analytic confidence levels, and ethics. Analytic judgments that are passed to policy-makers are bound by important guidelines in these areas. The educational setting also offers opportunities for students to see the complexity of each of these areas, and to expand their mental frameworks. The core curriculum, coupled with classroom dialogue, results in healthy discourse between faculty and students that challenge and expand the students' mental frameworks.

The socialized way of knowing is linked to the social aspect of learning. This approach rests on the premise that the social context influences students' views. Using carefully constructed cohorts, NIU seeks to ensure cognitive diversity that enhances the social learning environment. This helps students understand how their classmates and their classmates' parent organizations approach problem sets, again stretching their mental frameworks. Understanding Mezirow's theoretical framework, faculty members in the role of facilitator can help bridge the gap between present understanding and newly acquired experiences that oftentimes lead to a disorienting dilemma, as mentioned earlier in the paper (Mezirow, 1997, 2000). This offers a wider perspective with which to enhance students' problem solving and critical thinking abilities.

The Capstone project and the thesis are the culminating academic experiences that allow each student to demonstrate critical thinking, innovation, and analytical problem solving in a cohort environment. The Capstone and thesis projects are geared towards the self-authoring way of knowing that is informed by reflections on core courses and electives, faculty and student discourse, and engagement with members of the Intelligence Community. Students in the self-authoring phase of the curriculum are now better equipped to step outside themselves and look at competing ideas or relationships. It is in this phase of the academic year that transformation becomes evident. Through a unique mix of instrumental, social, and self-authoring learning, NIU students reach higher stages of development.

Fostering Transformations in Intelligence Organizations

The Conditions of Transformation: Our scholars offer pointers for enhancing learners' development. Mezirow (1997, 2000) suggests guiding learners toward autonomy by helping them recognize biases and mental frames (their own and others'), helping them learn to redefine situations from a different point of view, and helping them be adept at discourse. Mezirow explains that growth begins with a disorienting dilemma, followed by reflection and discourse. These conditions help a learner become aware of his or her underlying beliefs (assumptions). This awareness can help the individual form a new

understanding, expanding his or her mental frameworks. Analytic work environments can be shaped to maximize the learning potential of the conditions already present. The below suggestions can be implemented in every-day workplaces.

Drago-Severson (2004) recommends educators should consider each learner's own way of knowing, challenging and supporting that learner in a developmentally-appropriate manner. She calls this simultaneous challenge and support a holding environment. Methods of creating a holding environment at the office could include the following four areas of suggestion.

One, establish conditions for asking questions and exploring how a phenomenon or issue works, for exploring its context, and for analysts to connect with collaborative partners. Expect analysts to make meaning of their experiences inside and outside of work. Pay attention to disorienting dilemmas; open up safe, constructive opportunities to talk about it (Drago-Severson, 2004). Encourage shared meaning-making in trusting settings. Two, establish a culture of support and helpfulness, in part by emphasizing collaborative practices and de-emphasizing competitive and individualistic metrics (Grant, 2013).

The third suggestion is a method of achieving the first two. Create a community of connection between learners (a cohort). Creating a cohort setting can be very effective; learners support each other and provide opportunities for sharing perspectives through discourse. This is a unique component in the undergraduate program at NIU; the students have become tightly connected to their cohort by the time they immerse themselves in the intense challenges of their Capstone project presentations. A cohort in a work setting would be a similarly tightly-knit group of people who develop familiarity and trust with each other. A practice that has been effective for organizations focused on employee development has included routine work-group discussion before, during or after projects or presentations. The attention would be on the purpose of the project, ways of moving ahead, and constructive assessment of how it went (Kegan and Lahey, 2016).

The fourth area can be difficult to justify when time or money are short, but is well worth the investment. Allow opportunity for analysts to travel or attend events that are related to their field, though

might not be directly part of today's work assignments, if they will offer expanded perspectives.

Analysts, like all adult learners, should be challenged and supported at the same time (Drago-Severson, 2004). Opportunities for growth can be provided in the every-day settings in which analysis is conducted, under certain conditions. We see this growth as essential for success in intelligence work; intelligence can only keep up with security threats if analysts can reframe their understandings while the world keeps spinning.

References:

1. Cockayne, James, (2016). *Hidden Power: The Strategic Logic of Organized Crime*. London: Hurst & Company.

2. Danzig, R., Allen, J., DePoy, P., Disbrow, L., Gosler, J., Haines, A., Locklear III, S., Miller, J., Stavridis, J., Stockton, P., and Work, R., (2018). *A Preface to Strategy: The Foundations of American National Security*. Johns Hopkins Applied Physics Laboratory.

3. Drago-Severson, E., (2004). *Becoming Adult Learners*. New York: Teachers College Press.

4. Grant, A., (2013). Givers Take All: The Hidden Dimensions of Corporate Culture. *The McKinsey Quarterly*, April.

5. Heuer, R. Jr., (1999). *Psychology of Intelligence Analysis*. CIA: Centre for the Study of Intelligence.

6. Hoggan, C. D., (2016). Transformative Learning as a Metatheory: Definition, Criteria, and Typology. *Adult Education Quarterly*, 66(1), 57–75.

7. Kahneman, D., (2011). *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.

8. Kegan, R., (2000). "What 'Form' Transforms? A Constructive Developmental Approach to Transformative Learning" in *Learning as Transformation: Critical Perspectives on a Theory in Progress, 1st Ed*., ed. Jack Mezirow. San Francisco: Jossey-Bass.

9. Kegan, R. and Lahey, L., (2016). *An Everyone Culture: Becoming a Deliberately Developmental Organization*. Boston: Harvard Business Review Press.

10. Kerbel, J., (2004). *Thinking Straight: Cognitive Bias in the US Debate about China*. CIA Center for the Study of Intelligence,

https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article03.html# accessed 02-18-2019.

11. Lowenthal, M., (2017). *Intelligence: From Secrets to Policy.* 7th Ed. Los Angeles: CQ Press.

12. Marrin, S., (2011). *Improving intelligence analysis: Bridging the gap between scholarship and practice.* New York: Routledge.

13. Marrin, S., (2011). *Improving intelligence analysis: Bridging the gap between scholarship and practice.* New York: Routledge.

14. Mezirow, J., (1997). "Transformative Learning: Theory to Practice." *New Directions for Adult and Continuing Education*, 74, 5-12.

15. Mezirow, J., (2000). *Learning as Transformation: Critical Perspectives on a Theory in Progress,* 1st ed. San Francisco: Jossey-Bass.

16. Office of the Director of National Intelligence. (2015). *Intelligence Community Directive 203: Analytic Standards*. McLean, VA.

17. Zegart, A., (2007). *Spying Blind: the CIA, the FBI, and the Origins of 9/11*. Princeton: Princeton University Press.

REGULATORY INTELLIGENCE TRAINING – A NEW FRONTIER FOR EDUCATORS

Neil QUARMBY*

Abstract

Education in intelligence and analysis has traditionally been oriented towards national security and more recently law enforcement. Reforms in personal and business behaviours are driving the need for improved regulatory systems in the Western world, which is also creating an imperative to build professional intelligence capability and networks across new areas of government and industry.

Keywords: *intelligence, regulation, supervision, compliance, prevention, risk.*

Introduction

Regulation, licensing, supervision, monitoring, inspection, compliance, safety investigation, accreditation … all representative of the broad church of government and organisational controls reflected in this paper as "Regulation". They all have a core determinant: assessing and monitoring the performance of participants in a government defined area of risk that has socially or legally sanctioned rules for appropriate behaviours. The aim: to prevent harms to people and business. (Sparrow, 2008)

* Neil Quarmby is the chief executive of Intelligence Rising, a consultancy and online training company in intelligence. His career spans over twenty years in Defence intelligence, law enforcement intelligence, and he has led three regulators in three different government sectors. He has published two books on intelligence and is affiliated with Macquarie University, Australia. He can be contacted through contact@intelligencerising.com.

The scale and complexity of regulation on peoples' lives is daunting. The effectiveness of regulatory controls has even become a key measure of a nation's status as a modern economy. Hence there can be an apparently limitless number of regulators, ranging from several staff to major government departments. The scale of preventable harm is also daunting – and touches everyone daily in the costs of living, doing business and in injury and death.

Contemporary intelligence thinking is being propelled into the world of regulation by: negative performance reviews of regulators; new leadership intent on achieving a sense of public value; the idea of connected government; and demands for more efficient targeting of resources at risks. Yet there remain sizeable barriers in regulation to intelligence capacity-building. Some of these barriers are legislated while others relate to the nature and scale of the data held by regulators. However, the most significant barrier relates to cultures within regulators themselves and the government they provide assurance services to.

One key issue is that regulators are not supported academically – like national security and law enforcement – as there is no active debate on targeting intelligence practices, detection thresholds, surveillance, and counterintelligence. There is a general absence of intelligence as a discipline across the broad expanse of regulatory entities. Globally, academic, judicial and government reviews of regulatory failure rarely mention the word intelligence. Recent reviews of failures of financial and banking system oversight (supervision) observe failures in monitoring, targeting, indications and warnings, and threat assessment of the culture of financial organisations. Regulators have been publically flogged for their focus on financial performance data. Yet the term intelligence is rarely used in the findings of failure.[1]

Hence, this paper foresees a growing demand on the intelligence profession over the next twenty years for core skills and expertise to be transitioned into the varied arms of state regulation and commercial compliance; similar to the journey started by law enforcement internationally twenty years ago. The paper explores the number of

[1] An example capturing a range of reviews of the performance of European and Australian regulators is in Hane (2019, pp. 337-385).

inherent cultural and structural barriers to the easy adoption of intelligence-led decision-making in this broad sector and presents some observations on the types of focus areas to address this new and exciting challenge for education and training systems.

Definition

For the purposes of this paper, the term 'regulatory intelligence' can be viewed as: involving the systematic collection, identification and analysis of behaviour, important hazards, risks, or patterns of non-compliance for regulatory decisions. (Sparrow, 2000, p. 100. Quarmby & Young, 2010, pp. 3-4)

The world of regulation

Taking a helicopter view of regulation, the scope can be viewed as too large for a simple education framework. The scale of law enforcement tends to outweigh national security and the scale of regulation outweighs law enforcement in fully modernised countries. All markets and sectors have rules regulating interaction between private actors or the interaction between private actors and government. Regulations also cover how government departments and agencies interact between themselves – and hence there may even be government watchdogs oversighting government officials. In the traditional national security view of intelligence, the less trusted states are those with few internal, public, regulatory controls in place.

Modern economies have a plethora of ombudsman, audit, complaints management, protection, security, and review bodies. The scope can also be expanded to include self-regulating market bodies such as professional associations (peak bodies and representative bodies) that accredit members and investigate performance; such as medical practitioner associations and legal professional bodies. In some cases, these representative bodies may themselves be subject to government regulation.

In the work-place, there are code-of-conduct measures imposed by employers subject to varying levels of investigation. In turn, there are appeals mechanisms for complaints against such systems, subject to

review by external intermediary and/or investigative bodies. Just when you think you can escape such codified behaviour, your home may also have rules and standards – some of which are self-imposed but others may be highly codified by society; for example, how you get rid of your waste.

Regulators obtain and generate staggering amounts of information and data needed to support the decisions they make to reduce harm. 'Harm' is used in this paper in the broadest of senses and relates to the primary prevention purpose of all regulators. Harm may refer to the impact of poor behaviours on systems integrity, travel controls, identity security, market equity and integrity, public health and safety, environmental stewardship, corruption control, personal integrity, and transaction integrity. (Sparrow, 2008, pp. 1-2) Reputational harm leading to loss of public confidence in a market sector is also often a crucial factor; for example in banking and business behaviours.

The complexity multiplies on a scale of national harm. From a social perspective, more people die in preventable circumstances in the domain of regulation than in the domain of crime (Quarmby 2018, p. 5). On a financial scale, more tax-dollars are lost to noncompliance and incorrect or inappropriate practices than criminality. The global financial crisis of 2007-09 was attributed in part to the many regulators' reduction in regulatory oversight and subsequent failures "to monitor individual financial institutions and individuals" (Black, 2011, p. 1). A recent Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry in Australia, reflected on previous work done in improving the supervision of banks in Europe; especially in the Netherlands and under the auspices of the G20. The Royal Commission found significant weaknesses in the regulatory system leading to financial and social harms. The result: loss of confidence in the banking sector and billions of dollars required to be paid in reparations. (Hane 2019, p. 37)

While the Commission identified regulatory failures in monitoring and detection, the word 'intelligence' is never used in the Royal Commission's findings – as it would be if the problem was deemed a national security issue. In reflecting on this failure, the

Commission notes the absence of learning from international experience. For example, the financial crisis in Dutch banks led to the regulatory arm of the De Nederlandsche Bank (DNB) introducing a regime of assessments of behaviour and culture in the institutions within its regulatory coverage. The DNB's program has been developed on the idea that '[c]ulture and behaviour are essential elements for financial and prudential supervision, since the behaviour and culture of a financial organisation influence its financial and organisational performance'. By 2015, the DNB conducted 52 assessments of 'banks, insurance companies, pension funds and trust offices'. Most assessments focused on senior management. According to the DNB, more than half of the boards assessed 'showed serious problems with regard to their board culture'. (Hane 2019, pp. 377-9)

Drivers for investment in intelligence tradecraft

Given this sense of harm and the clear relevance of intelligence tradecraft, it remains surprising that few areas of regulation appear to attract serious intelligence investment. Certainly, revenue regulation and assuring welfare payments tends to attract investment by government in control and targeting measures due to the considerable impacts on the public purse. In Australia, the government revenue regulator (the Australian Tax Office [ATO]) identifies a key task is to work "with other Australian Government agencies to deliver services; share data, intelligence and expertise; and participate in multi-agency taskforces." The ATO reports it has 115 Memorandums of Understanding (MOUs) in place with other Australian government agencies and bodies (federal, state, territory and local) to manage this function. (Commissioner of Taxation, Annual report, p. 17)

Finance and Tax regimes have tended to attract a greater proportion of intelligence expertise due to undercurrents of crime and the national security agenda. Other major regulatory arms with significant harm issues such as Health regulation are lagging internationally. 'Health intelligence' more often means statistics on a morbidity factor. While there are more financial costs and human costs arising from failure in Health regulation than there will ever be in national security and revenue regulation, this regulatory sector tends to

remain impervious to contemporary intelligence practices, and hence investment is data-centric and meaning-limited.

The value of centralised intelligence centres, able to acquire and fuse multi-source information for the benefit of connected intelligence capability in supported business lines, is ingrained in national security and has come late to law enforcement. In the US – with some 17,000 law enforcement bodies (including very many regulatory bodies) – there are approximately 75 fusion centres attempting to share information and intelligence across the security, crime and public safety divides (Ratcliffe 2016, p. 21). Such centres do not occur naturally in regulation without a push from national security entities or crime fighting bodies. There remain significant barriers to implementing such innovative ideas within regulatory circles.

As a sample, the 'public face' of 58 international regulators was reviewed by the author as to whether they advertised their regulatory approach as incorporating intelligence practices. 16 out of 58 had a publically stated approach to operations that intelligence practitioners could vaguely associate with (Quarmby 2018, p. 51). Only three of the 58 regulators – at the time of review – had a publically stated approach to targeting behaviour that appears to be in tune with contemporary intelligence-led theory and practice (Quarmby 2018, p. 53).

The public would assume that, where regulators operated in similar jurisdictions (for example with common participants and like harms), regulators would adopt consistent approaches to targeting harm. In national security circles this is often referred to as interoperability. However, the study showed that consistency should not be assumed. Dissimilar regulatory philosophy and approaches between agencies tends to create barriers to sharing information and intelligence. Meaning that - even in like sectors where they have to deal with a common problem – regulators struggle to share crucial intelligence without the same language to assess and define problems (Quarmby 2018, p. 52).

So … what is different about regulatory intelligence for educators of intelligence?

The educational institutions are absent: Much of the world's contemporary education of intelligence has its foundations in international relations. Early academic texts placed intelligence firmly in the domain of supporting decisions about foreign threats. Much of debate therefore tends to be about how independent the intelligence system should be from the policy-makers (Davis, The Kent-Kendall Debate of 1949). Hence the rationale for intelligence education is usually perceived in the Machiavellian tradition of understanding inter and intra state threats, and protections for people in a national security construct. The academic pursuit becomes one of understanding whether intelligence is best understood as a manifestation of realpolitik, neo liberal perspectives, neo Marxist/culturalism views, or even through the recent constructivists who have a more practical, inter-state problem-solving approach to education. The shape of such academic pursuit is strategic in nature. Given, the vast majority of intelligence officer jobs are tactical, such an academic prism is only viable where the core of intelligence officer tradecraft exists in the training regimes of those agencies affiliated with national security.[2] Academia then provides a more foundational, strategic capacity outcome. This education structure allows education in academia to focus on strategic intelligence roles and analytical tools relevant for the study of wicked international relations problems.

That is the theory … however; the nature of academic tradition can confuse the theory. In the US, intelligence education arose to assist the growth of large numbers of strategic analysts from within the international politics domain and later gained traction in criminology studies. In Australasia, intelligence education was initially driven by Universities' Criminal and Justice Departments from the 1990s, with then a later take-up in International Politics Departments. Here the

[2] Numerous works by Bob de Graaff on intelligence highlight this tradition through Europe. One work notes a driver from the military to enhance academic intelligence training in the Netherlands and not to duplicate the training work of the services (de Graaff 2013, p. 88-9).

tradition is more social and humanist than political.[3] More recently Information Technology Departments are growing their intelligence and counterintelligence expertise to ultimately challenge the intellectual ownership of intelligence – but based on a scientific and mathematical tradition.

The nature of internal to agency training capacity also confuses the education continuum. For example, there has been a general absence of a training capability within justice/policing agencies to grow intelligence officers. Where internal-to-agency intelligence training exists, it may focus on the type of IT analytical support tools used by that enforcement arm. Many Western policing departments/agencies may not allow intelligence officers to be involved in what are the traditional collection practices of intelligence. Rather, their intelligence staff are contained to only analytical roles.

Hence, there has been a natural problem in university justice courses attempting to adopt the structured analytical approaches used in national security without pre-existing tactical intelligence and decision-making DNA in place within the police forces serviced. The outcome is cognitive dissonance. For example, police workplaces not liking to employ intelligence students who have been focussed on the analysis of strategic problems far removed from their daily tactical work in criminal intelligence. Also the students themselves may not be able to relate academic study to the volume of tactical work faced by them in their justice or enforcement roles. For both employer and employee, the intelligence cycle may not be considered relevant – only the analytical segment.

While there are educational issues for law enforcement in linking their own internal training to the broader education offering of universities, the problem compounds for regulators who have little internal training and no university departmental alignment. The growing number of regulators seeking to professionally develop their analytics staff has few places to turn. What is worse, is the converging influence of data analytics and a pervasive view that regulators may only make decisions on data or evidence, and means regulators seek to

[3] For a history of the rise of intelligence practices in law enforcement see Ratcliffe (2016).

fill this void through education in the data sciences. Hence, many information systems or legal/justice studies departments in universities are seizing the education ground on intelligence; however, the view of intelligence is one of managing the system to share data, to store data, to match and collate data, and to report data.

Poor design in regulation does not help! Regulatory systems are characterised by the law that authorises action, the participants being regulated, the capabilities of the regulated, others impacted by regulation, the policy and political stewards of the system, the legal sector and representative groups of various parties. The interplay between these various elements is often referred to as the 'regulatory scheme'. (Quarmby 2018, pp. 66-68)

The design of regulatory schemes drives a lot of regulatory culture that flows through operations and intelligence. It is interesting that medical practitioners defrauding or conducting noncompliant billing in the USA are targeted by the FBI within an enforcement context. In Australia, the same targeting is conducted by a non-statutory regulator (and one that bounces between polar views of itself as a regulator or an internal public service assurance body). Hence the design itself sends a clear message as to public acceptability of what is tolerated. Where corruption and black-markets operate in normal business transactions, less meaningful regulatory systems will be in-place and certainly no regulatory intelligence system will be in-place.

A well designed regulatory scheme would include the right level of information access to enable the regulator to monitor performance and behaviour. Unfortunately, very few regulatory schemes are designed with intelligence functions in mind. Most have an overriding focus on how specific enforcement tools or powers can be used. This is important work, but tends to leave regulators with authorising environments representative of 20th century law enforcement approaches and not 21st century contemporary regulatory practices. Worse case, design inhibits the regulator's ability from the outset to monitor those areas of behaviours and risks likely to generate the most harm.

Sparrow in his seminal work on the Character of Harms (Sparrow 2008), outlines a number of approaches regulators take from being: Type 1 prescriptive and rules-based; to Type 4 no real oversight;

through various iterations between these polar opposites. These models can be characterized as shown in the figure below.

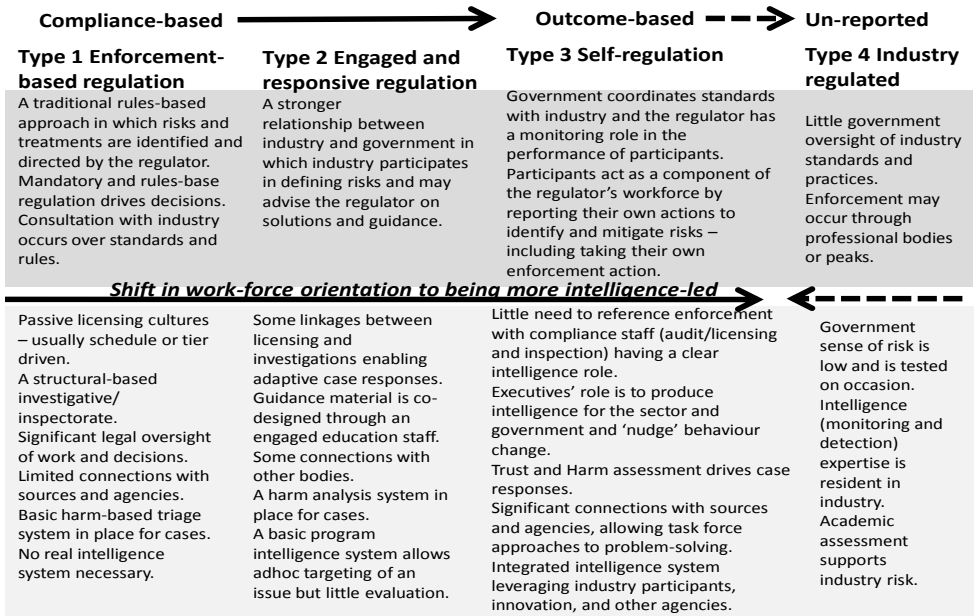


Figure 1: Stewardship models of regulation taken from Quarmby (2018, p. 109).

These models are especially useful in starting the discussion about the nature, type and scope of capacity building needed in the regulator. Most regulators and scheme stewards will aspire to the third model. They are wary of the fourth due to systemic failures and lack of transparency and protections. They are wary of the first due to the connotations of being anti-business and pro-red tape. Often the models are proposed simplistically; that is, a regulator can only be one or the other. In the author's experience most regulators will have market segments necessitating a variance in approach across this scale. At the same time, it is the author's experience that most regulators cannot clearly articulate (as a unified voice) what approach they have to these different market segments.

The most important and fundamental aspect to these four models that is lost in most contemporary literature is that the workforce as well as the culture changes markedly as regulators shifts from Type 1 to 4. These implications are covered in detail in *Intelligence in Regulation* (Quarmby 2018, pp. 109-122). Suffice for educators to know they need to discuss the shape of intelligence arising from the culture of the regulator and the key shifts in intelligence work depending on this culture. For example, a critical shift for regulators seeking to be more of a Type 3 regulator is the necessity to understand what good behaviour looks like and how best to adjust it and reinforce it. National security and police intelligence officers have extensive professional expertise in analysing bad behaviours; but good behaviour? Not so much. National security success can be measured in identifying and dealing with threats. Regulatory success can be measured in expanding the growth of the compliant and better practice participants to achieve a social end-state in which the regulator is no longer required and behaviour is self-policed and self-reinforcing.

Transparency and the relationship with policy making: There are two other major departures from traditional intelligence perspectives worth noting. The first is the element of transparency. National security and police intelligence operates in a carefully controlled environment due to very real counterintelligence risks and due to the sensitive nature of many sources. In regulation, often the most important tool to sustain good behaviour is through public engagement and public reporting on performance. Indeed there is a public expectation for regulators to report on the performance of their jurisdiction and the types of harm manifesting. Hence in Type 3 regulator there should be a clear shift to visibility and openness that is often uncomfortable for traditional compliance and intelligence staff.

The second is the relationship to policy. As noted earlier, traditional academic study into intelligence fusses over the independence of the intelligence officer from the policy officer. This means there is little doctrinal support for intelligence reports providing recommendations. In regulation the issue is compounded as often it is weaknesses in regulatory response or policy controls that allow noncompliant behaviours to manifest. Deeming government policy to

be the most important threat factor can be career limiting; however, very necessary in regulatory intelligence work!

Barriers to be understood by educators

Organisational culture and the absence of decision-making DNA: To explore approaches to educate intelligence officers working in the regulatory and compliance world, academic institutions and trainers need to understand the barriers to employing such expertise. These are covered at length in Intelligence in Regulation (Quarmby 2018, pp. 7-64). In short, these barriers include the conservative culture of many regulators. Passive rules-based obsession is not normally conducive to encouraging the creativity and networking necessary for a contemporary intelligence culture. Also the data-centric nature of regulators tends to confuse contemporary intelligence thinking with that of data analytics and business intelligence.

For many regulators, understanding the intelligence function is problematic because of the absence of 'direction'. Regulatory decision-making is often case specific. Hence the term 'strategic' may be used in regulators for those big cases that have reputational risks. In many regulators, key case decisions related to licensing, audit programs, the use of powers, campaigning and enforcement responses are made at the highest levels. Such decision-making is often (and quite necessarily) guarded by legally formatted and contestable process requiring hard evidence. Speculation may be spurned.

Where there is little organisational space for strategic and operational level decisions, the intelligence function is most often subsumed by business intelligence or data analytics functions. Here, analysis is reduced to reporting known statistics and may even be overshadowed by internal performance reporting. Hence, creative innovators seeking to source new data and information get frustrated in regulators; especially where the perception internally is that additional information from other sources cannot be used in legally defined decision processes (Quarmby, 2018 pp. 44-5).

Where regulators do recognise the value of other sources, intelligence may be considered an IT problem; about the sourcing and integration of data. This may lead to structural and functional

uncertainty as to whether analysis of data is best placed as a corporate rather than a business function, and also may lead to expensive solutions for otherwise simple problems.

For educators, an intelligence capability needs to be present in regulators for the type of behavioural analysis that will drive successful domestic policy and targeting decisions.

- It needs to be present to support strategic thinking on the future connections between law reform, public value shifts, and operational capability development.
- It needs to be present to assist decision-makers seeking an appropriate response to a behavioural problem (operational decision-making) within their jurisdiction.
- It needs to be present to allow compliance case management to select and use the appropriate tool in responding to a case (tactical intelligence).

Absence of scholarly support: The academic view of regulation is yet to mature and explore the concept of improving decision-making through enhanced intelligence systems. Rather the focus to date has been on responding at the case/incident level (Quarmby 2018, p. 46). The intellectual discourse for intelligence in regulation is non-existent in comparison to both law enforcement and national security. In the few volumes of good academic writing on regulation, there is very little mention of intelligence and decision support. Even Sparrow's seminal works are light on the subject (Sparrow 2000 and 2008). Baldwin and Black (2007) also comment on this general literary absence.

Recruitment of people into regulatory positions often follows the literal interpretation of the authorising environment and not the subtleties of creative problem-solving imposed by contemporary thinking. Hence, regulators tend to recruit from industry or recruit operational people specific to their statutory functions of audit, inspection, complaints handling, investigation, information management etc. Complicating matters, there is very little in the way of educational pathways for regulators through universities or public service training regimes. Such pathways could assist people from various backgrounds to professionalise as a regulatory leader.

Within such a context, it is easy to see why many regulators have internal cultures not conducive to contemporary intelligence design and indeed how they get caught 'not knowing' what is clear and obvious.

The most public failures internationally include the 2007-09 Global Financial Crisis and the Deepwater Horizon drilling disaster in the US in 2010 and both have been extensively examined. As Julia Black notes: *"The nature and reasons for the failures are extensive, but were largely common to regulators and market participants alike. Many of these were cognitive: fundamental failures of regulators as to how the markets were operating…"* (Black, 2011)

Every country has these regulatory failures and lack of knowledge or ability to harness information is often a key symptom. Underneath, there is often more of a dynamic of poor decision-making that has precluded investment in contemporary intelligence.

With such evident and catastrophic failures, why the lack of interest from intelligence and academic professions? Low likelihood + high consequence events are the core analytical grist of the national security intelligence arena. These are often attractive and intellectually stimulating for many analytically minded people. Conversely, the daily grist of analysing our own behaviours that undermine our ability to govern our own transactions is far less intellectually stimulating.

An absence of tradecraft: 'Direction' and artistry in driving an intelligence cycle demands intelligence trade craft in collection management. In national security, education in this art is usually the accountability of service or intelligence agency internal training programs. Hence – as noted earlier – there is foundation education that can rationalise the academic focus on strategic international problem-solving along a broader training to education continuum.

In regulation and law enforcement, the academia focus on training staff as just strategic analysts can be calamitous for their burgeoning intelligence profession.

Intelligence officers will, by their nature, always search for what is not known. However, in law enforcement and regulation internationally, analysts are required to collate information at hand; within a problem set for them. Analysts are rarely let out to collect; let

alone shape collection. Analysts become contained within the organisational bias of their employ. Hence, broadening education and training systems to encourage tradecraft in planning and monitoring – by breadth and depth and driven by intelligent questions – is paramount.

Intelligence practitioners are trained to reduce intelligence requirements into a series of information requirements which are necessary for analysis and to answer the decision-need. What information is at hand is first considered and preliminary significance and meaning – as well as a gap analysis – occurs. Consideration is then given to the need to address gaps and how to most efficiently fill them. Use of other agencies is considered as well as pursuing sources through the operational arms. If such skills permeated regulation, where another agency has the information sought, then – in the spirit of red-tape reduction – participants in the scheme do not need to be levied with additional information checks. However, such approaches in regulation are rare or require extensive legal agreements. Given most information requirements in a regulator can be answered from within accessible data-sets, the default is usually not to bother with chasing other sources. However, often the key issue of behavioural motivation and causality is not easily derived from the information at hand and hence the core tenant of intelligence is lost.

The lack of clear thinking around this concept is usually at the heart of regulators suffering adverse reviews or 'missing something' (Quarmby 2018, Part 2). There will always be information gaps in regulatory knowledge requiring access to information not immediately available. The cost/benefits of resourcing collection against these gaps should be carefully considered and additional layers of collection tasking added.

Education in how intelligence systems can be designed for coverage (by both breadth and depth) is therefore very necessary. Many regulators check or validate behaviours based on a schedule or sample. A contemporary view of the concept of coverage implies a considered balance of resources (both external and internal) applied proportionately across the at-risk behaviours in the jurisdiction. The more at-risk (higher impact) behaviours have more frequent or tailored

monitoring, while there is still capacity held aside to check on less frequent or less interactive participants (Quarmby 2018, pp. 129-131).

The concept of depth is inherently tied to the concept of breadth in regulatory intelligence. Monitoring has to have a sense of 'how deep are we trawling?' connected to 'how wide are we casting the surveillance net?'

An absence of tradecraft in collection planning is exacerbated by an absence in tradecraft in operational collection and exploitation of sources. In the human intelligence domain, regulators rely heavily on people and contacts for information that provide texture to otherwise grey transaction information and data. The tip-off, the whistle-blower, the people the inspector talks to on the work-site, the union official, the lawyer, the family members, the social networking group; all contribute essential intelligence for regulators. A contemporary intelligence system will enable a framework around human intelligence; set rules and collection management accountabilities. However, few regulators have professionalised the management of sources; hence, valuable insights and sources can be lost. Similarly, the transferable communications intelligence tradecraft for regulators lies in social media exploitation. Yet few invest in the skillsets to exploit new age media (Quarmby 2018, p. 131-133).

A critical footnote in this absence of tradecraft is that most regulators (if they have an intelligence function) are often single-source intelligence agencies. As noted previously the extent of data collection, data myopia and organisational culture lend regulators to only analyse what they know, based on their preferred source. For some this involves a leaning towards reliance on their transaction data. For others, action only occurs from public tip-offs. The narrow idea of intelligence as **a process** of converting information into intelligence satisfactorily fits in with such myopic cultures. The concept of being intelligence-led is readily converted into the need for a few extra staff and an extra step in the call centre or in the data extract and analysis process. The main point becomes lost in the single-source preferences of the organisation; the main point being: 'what don't we know, how significant is it, and how can we collect it?'

Differences in analytical techniques: risk, threat and harm

Much of the analytical approaches taught in intelligence are relevant in regulation. There are, however, a number of terms or types of analytical lens worth highlighting.

Risk – is a term related to decisions – and has a consequence and likelihood (event-based) analytical construct. Risk language used across regulators tends to limit analysis and the employment of intelligence professionals. Intelligence investment needs to be focussed on expanding the regulator's understanding of harms and trust/threat levels, as well as trends and patterns in behaviour. This is best stylised as 'at-risk' behaviours. Without this simple construct, the term risk can be confused with the concept of the risk of noncompliance; in other words, the risk of breaking a rule. As the failure of banking regulation internationally has uncovered, often the core at-risk behaviour to be assessed is more the organisational intent or the culture, and this is not an arbitrary rules-based measure (Quarmby 2018, pp. 59-61).

Harm is a term more relevant to behaviours targeted by regulators where the harm manifests as impacts in the domains of the social, economic, political/reputational, equity, personal, real/perceived… (and is therefore public value-based). The term 'triage' is used in regulation as the most basic form of analysis for harm.

Threat / trust – are interchangeable analytical lens in regulation segmenting those participants in the scheme likely to commit the harm. Some regulators may refer to participant "conduct" or "attitude to compliance". As a minimum it includes analysis of history, individuals, governance, associations, leadership, workers, market segments, stakeholders, interest groups etc. (and is therefore entity-based).

Three analytical approaches tend to dominate regulatory intelligence work:

- Statistical analysis – where there are patterns available in transaction data;
- Typology/morphological analysis – where there are no statistical patterns in data but the various component parts of 'problems' cross-connecting behaviours with identifiable actions, can be grouped and considered;

- Profiling – a combination of statistical and typology providing current and background assessment of the performance of an entity. Usually includes comparative indicators aligned by designated attributes. More complex profiling includes association analysis and projections of behaviour.

The following table provides an example of the various components of a profile of a commercial entity subject to a number of performance standards within a jurisdiction. The example fuses the concept of morphological, statistical and trust analysis noted above.

<table>
<tr><th>Attribute</th><th>Assessment and Metrics</th><th>So What?</th><th>Now What?</th></tr>
<tr><td>Governance</td><td>Better practice</td><td rowspan="4">Market sector importance, viability, strengths and weaknesses Associated with the Regulator's current areas of interest?</td><td rowspan="8">Desired behavioural change
• Entity level
• Sector level
Tone, timing and tempo of engagement</td></tr>
<tr><td>Probity</td><td>History</td></tr>
<tr><td>Business performance</td><td>Statistics</td></tr>
<tr><td>Financial performance</td><td>Statistics</td></tr>
<tr><td>Safety or harm to people or markets</td><td>Events and system quality, complaints</td><td rowspan="4">Trust and Harm
Real or projected?
Known or unknown?
Comparative or unique?
Impact on regulatory or scheme reputation?</td></tr>
<tr><td>Reporting and regulatory responsiveness</td><td>Statistics
Other inputs</td></tr>
<tr><td>Associations</td><td>Association analysis</td></tr>
<tr><td>Intent and investment in better practice (including regulation)</td><td>Futures</td></tr>
</table>

Table 1: Systems, attributes and morphological analysis (Quarmby 2018, p. 157)

Conclusion

With the rising demand for the cross-pollination of intelligence skill-sets and tradecraft from new sectors such as commercial competition intelligence, compliance, risk and regulation, there is scope for new innovative service offerings supplementing traditional academic courses. Training needs can be, to some extent, met online. The more enduring education provided by Universities could expand the environmental constructs of the intelligence course beyond the traditional domains of national security.

There is little education on offer internationally for regulators and especially for intelligence functions in regulation. The test for academia is managing the ownership of intelligence professional education across otherwise competing faculties. In the meantime, in-house training will remain central until education systems catch up with the demand.

Some thoughts tying training together with the other workforce planning notes above are contained in the following table.

	STRATEGIC	**OPERATIONAL**	**TACTICAL**
Training Requirements (Level Specific)	**Senior Analysts and Managers only:** • Managing in intelligence • Influencing and Reporting • Performance measurement • The art of regulation • Public value **Analysts and Senior Analysts and Managers only:** • Strategic	**For Senior Analysts and Managers only:** • Managing data analysis, mining and sharing • Business intelligence • Influencing and Reporting • Performance measurement • The art of regulation • Requirements and collection management	**For Senior Analysts:** • Managing entity analysis • Influencing and Target Packaging • Performance measurement • Requirements and collection management **For Analysts and Senior Analysts only:** • Advanced entity analysis and association

	assessment processes **Induction for all**: • Intelligence cycle • Basic collation, analysis and reporting techniques	**Analysts and Senior Analysts only:** • Advanced analysis techniques – statistical, systems and morphological modelling • Harm and trust analysis • Specialist tools – eg geospatial • Collection techniques • Source development **Induction for all:** • Intelligence cycle • Basic collation, analysis and reporting techniques	techniques • Profiling • Harm and trust • Specialist tools • Collection techniques – source exploitation and management **Induction for all:** • Intelligence cycle • Basic collation, analysis and reporting techniques

Table 2: Intelligence training needs in regulation (Quarmby 2018, p. 170)

References:

1. Ayres, I., Braithwaite, J., (1992). *Responsive Regulation: Transcending the Deregulation Debate*, Oxford University Press.

2. Baldwin, R., Black, J., (2007). *Really Responsive Regulation*, LSE Law Society and Economy Working Papers 15/2007, London School of Economics and Political Science Law Department.

3. Black, J., (2011). *Learning from Failures: New Governance techniques and the financial crisis*, Warwick University and Law Commission Symposium, September 2011.

4. Commissioner of Taxation (2015): Annual report 2014–2015, Part 02.

5. Davenport, T.H., Harris J.G., (2007). *Competing on analytics: The new science of winning*. Boston: Harvard Business School Press.

6. Davis, J., *The Kent-Kendall Debate of 1949*, Analysis and Policy, https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/Fvol35no2/2Fpdf/2Fv35i2a06p.pdf, downloaded 29 April 2019.

7. De Graaff, Bob, (2013). "Training Intelligence Producers and Consumers for the Future: The Dutch Approach", in *Journal of Strategic Security*, 6, no. 3 Suppl. 2013.

8. Freiberg, A., (2010). *The Tools of Regulation*. Annandale: The Federation Press.

9. Hane, K. M., (2019). *Royal Commission into Misconduct in the Banking*, Superannuation and Financial Services Industry, Final Report Vol 1. Commonwealth of Australia 1 Feb 2019, https://financialservices.royalcommission.gov.au/Pages/reports.aspx#final.

10. Ivec, M., Braithwaite, V., (2015). *Applications of Responsive Regulatory Theory in Australia and Overseas: Update*, Australian National University, Regulatory Institutions Network, Occasional Paper 23, March 2015.

11. Moore, M.H., (2013). *Recognising Public Value*. Cambridge: Harvard University Press.

12. Quarmby, N and Young, L.J. (2010). *Managing Intelligence, the art of influence*. The Federation Press, 2010.

13. Quarmby, N., (2019). *Intelligence in Regulation*. The Federation Press, Sydney Australia.

14. Ratcliffe, J., (2004). *Strategic Thinking in Criminal Intelligence*. The Federation Press, Annandale Australia.

15. Ratcliffe, J., (2016). *Intelligence-led Policing*, Routledge, New York 2nd Edition.

16. Sparrow, M.K., (2000). *The regulatory craft: Controlling risks, solving problems and managing compliance*. Washington DC: Brookings Institute Press.

17. Sparrow, M.K., (2008). *The character of harms: operational challenges in control*. Cambridge: Cambridge University Press.

18. Thaler, R.H., Sunstein, (2008). *C.R. Nudge: Improving decisions about health, wealth, and happiness*, Penguin.

CASE STUDIES IN TEACHING INTELLIGENCE: PROS AND CONS

Florian COLDEA*

Abstract

Intelligence is as much a profession as it is a discipline, as it is the gathering of information and the information itself. Intelligence is both a product and a process. It has a specific jargon, working methodologies, specific knowledge, and its own doctrines, theorizing it; it has its own means and methods of work and has grown into a fully-fledged academic field. Strategic intelligence is constantly trying to get straight two fundamental questions of the activity: what is its purpose, and what are its methods. The rest are a myriad of adjacent questions regarding objectives, how they are selected, what are the terminological details, its history, its limits etc.

Keywords*: intelligence education, theory, practice, case-studies, guidelines.*

Introduction

One of the foremost requests nearly every intelligence student has, from the first weeks of study, is that teachers support every theoretical enterprise with consistent case-studies, specific examples illustrating theory, not lacking a dose of sensationalism in revealing intelligences` insight into sometimes high profile cases, and maybe a different perspective from the one publicly known. And it is only natural to expect to learn from the lessons of the past and to pair theory and empiricism for a more efficient learning process.

However, my personal experience is that students are only partly content with references to case studies of successes or failures of other countries` intelligence, instead stressing a need to be more familiar with local intelligence`s activity. Both situations are not

* Lieutenant General (r) Associate Professor Dr. within "Mihai Viteazul" National Intelligence Academy, Romania.

without difficulties for intelligence academics, and even more so for scholars with extensive practical experience gained in years of work in the field. And some of those difficulties which I intend to explore are related to the very familiar challenges current intelligence poses: in understanding external cases, there are constraints pertaining to differences in political strategy, vision, and decision-making. The global and local strategic equation are also shifting factors and local interests might differ from global ones, which makes case-studies of external intelligence actions difficult to apply as pre-defined, borrowed recipes for local, individual problems. Regarding internal case-studies, there is, from one perspective, the aspect of secrecy; since Romanian intelligence is young, most of its experiences are still classified; from a different perspective, there are familiar challenges we all know too well: oversight can, in some instances, be used politically, generating a false public sentiment of illicit activities in intelligence; the legal framework in countries such as ours is frequently lacking and inadequate to current threats, leaving local intelligence with rather blunt working instruments.

Teaching intelligence: a few guidelines

Intelligence is as much a profession as it is a discipline, as it is the gathering of information and even the information. Intelligence is both a product and a process. It has a specific jargon, working methodologies, specific knowledge, and its own doctrines, theorizing it; it has its own means and methods of work and has grown into a fully-fledged academic field.

Strategic intelligence is constantly trying to get straight two fundamental questions of the activity: what is its purpose, and what are its methods. The rest are a myriad of adjacent questions regarding objectives, how they are selected, what are the terminological details, its history, its limits etc.

Loch Johnson, in his "Handbook of Intelligence Studies"(2017, p. 3), referred to intelligence as an **information product**, a **process** – formally known as the "intelligence cycle" –, a "**set of missions**" specific to secret services, and "a cluster of **people and organizations**" responsible for the former three missions.

Most **intelligence studies** programs in Romania and elsewhere are relatively new as an academic field or branch of social sciences and tend to employ a significant percentage of former and current intelligence officers as teachers[1]. And this, maybe also in order to avoid the well-known saying "those who can do, those who can`t teach". It is important to make intelligence teaching neither purely theoretical, nor a field for former professionals no longer connected to reality, a so-called "cemetery for the elephants", but a discipline well-adjusted in order to provide viable solutions for the overall national security.

The purpose of intelligence studies is twofold: to develop **academic research** in order to improve the intelligence process and product, and to **form generations of intelligence professionals**, while also striving to promote a security culture. In other words, intelligence studies are useful for a strategic development of intelligence, both from an academic and from a practical perspective.

It is important for students and for the development of this rather young field of education that those who teach a basically practical subject have actual insider knowledge of the subject, and in my opinion, intelligence is one of those fields where scientific research and practical experience need to be closely linked in order to make progress possible. Besides being an academic field, subject of necessary research, intelligence is a profession with requirements for **advanced skills**, and more than in other fields, the professionals and the researchers need to team up and sometimes even change roles in order to get the best of both worlds. Moreover, also using intelligence professionals in academic activity is a means of transferring expertise and institutional culture to future theoreticians and practitioners.

To use a metaphor, teaching intelligence without the practical side would be similar to teaching physics without doing any experiments, because intelligence is one of those disciplines which deals with concrete, empirical realities, therefore even sometimes described as empiricist (Budiansky, 2000); I do not entirely agree with

[1] For the purposes of the present paper, we maybe need to define intelligence studies as a branch of security studies (US) / strategic studies (UK), academic field which distinguished itself from military theory, according to some authors, and from International Relations, for others after World War II. It was obviously a field of interest for Romanian academia only late after the 1989 Revolution.

the characterization, because practice and theory are intertwined in intelligence, but this is further argument that practical experience and historical accounts are tantamount to the field.

Practitioners can be and often do become good theoreticians, due to their extended experience; there are many such examples, starting with authors such as Sherman Kent, CIA officer and father of intelligence analysis, Richards Heuer, CIA veteran intelligence analyst whose intended manual for government officials became, after 1999, one of the leading world studies in intelligence analysis, "The Psychology of Intelligence Analysis", to other equally famous contributors to theory due to their extensive practice, such as Sir David Omand, former chief of GCHQ, or Mark Lowenthall, assistant director for the CIA and staff director of the House Permanent Select Committee on Intelligence.

Intelligence and security studies became a priority for the Romanian academic environment only in the past two decades, but the field has known major developments, with its introduction as a distinct study area for several military institutions which form professionals, among which the "Mihai Viteazul" National Intelligence Academy, the Military Technical Academy, the academies of the terrestrial, naval, and air forces in Sibiu, Constanţa and Braşov, as well as the Bucharest Police Academy and "Carol I" National Defence University.

Civil higher education institutions such as the prestigious Babeş-Bolyai University in Cluj, the University of Bucharest, and the universities from Timişoara, Iaşi and Sibiu have extensive intelligence or security studies programs, offering from bachelor`s degrees to master`s and PhDs.

On one side, military academies have the advantage of forming intelligence and security specialists, while also ensuring appropriate conditions for discussions of classified information, and on the other side, civil universities allow for better awareness at society level about the national security risks, threats and vulnerabilities, helping to make safer security environment. Michael Warner, for example, would place intelligence studies in two different categories, in line with the dichotomy between civil and military education institutions, considering the acute need for secrecy. He referred to "intelligence studies (...) conducted one way **on the *outside*, with no official access**

to original records, and another way **on the *inside*, where a few scholars have intermittently enjoyed** sanctioned (if not always complete) **access to the extant documentation**" (Warner, 2017, p. 17).

I think that higher education dealing in intelligence and security should be open to exchanges, so teachers from the military academies would be also working in the civil ones and vice versa, which makes it possible to exchange valuable findings from both worlds. Cooperation in this regard, too, is the key to capacity building.

It is also significant that military academies and institutions, such as the National Intelligence Academy, are responsible for the **continuous education of intelligence officers**, a highly relevant function because it helps them grow professionally and further develop their career, thus enhancing overall institutional performance. In this regard, the professional development of intelligence personnel must also be a priority for intelligence managers, who need to be involved in finding innovative, motivating solutions for officers, as well as the means to rapidly develop training systems according to the objective institutional necessities of the intelligence agencies.

Case-studies: theoretical delimitations

The practical side of intelligence and the major contribution practitioners can bring to the field of intelligence studies starts from their actual experience, which can be a premise for in-depth analysis of actual situations, in other words, *case studies*.

The case study method of teaching actually consists of an **in-depth investigation of a single event**, ideally with data from several sources. According to some authors, case studying is "not a research technique or method in itself (...), but rather a strategy of approaching the socio-human, often from a qualitative point of view" (Chelcea, 2007, p. 598). In other authors' opinion, case studying is a research strategy, "an investigation through which a contemporaneous event is being researched in its real life context" (Chelcea, 2007, p. 598).

The actual advantage of case studying is that it starts with theory and returns to theory, testing it, enriching it and enhancing its empirical foundation. A case study can refer to a number of situations, starting

from an individual, a group, a community, a specific instance, an episode, event, phenomenon etc.

In order to be relevant, **a case study needs to either reveal a very typical situation, illustrating a theory, or a completely atypical one**. The essential is that cases need to be studied intensively and holistically, and exploration and understanding tends to precede over quantification and confirmation of theory.

According to Septimiu Chelcea (Chelcea, 2007, p. 601), case studies have three common traits:

- They refer to a **concrete research**;
- They study a **contemporary phenomenon** rather than a historical one;
- The respective phenomenon has a **complex structure**, being difficult to isolate from a specific context.

A specific advantage of case studies is that they can provide both quantitative and qualitative proofs, while allowing for a complex image of a quantum of interacting factors. Case studies were classified according to different criteria, such as cause-effect of their very subjects. In this regard, we can use causal or explanatory case-studies, descriptive or explorative ones, intrinsic – when they research a unique event/phenomenon, instrumental ones, when used to test a theory, and collective or multiple ones, when similar factors appear in several situations.

Another obvious benefit of case studying is the balance it brings between general or theoretical and empirical knowledge. They contribute to overall scientific development and can lead to new research, if used judiciously. They are useful in generating working hypothesis and confirm or infirming them in order to advance new theory.

Challenges in using case studies are, I think, obvious: **choosing a case-study cannot be done randomly**, but rather very carefully, in order to generate progress. Natural **biases** can pervert the choice of a case study, meaning that the researcher can be inclined to favour those particular case studies which confirm his theory and initial assumptions. It would obviously be more useful to case study situations offering counter-arguments to prevailing assumptions.

Maybe a good example of such – even unintentional – biases is in the award-winning book *Thinking Fast and Slow*, where Nobel-prize

winner Daniel Kahneman illustrates the way the human mind tends to short-circuit extensive reasoning in order to save energy and effort and confirm/apply previously known patterns. One simple and revealing example in this regard is that of the "Librarian or Farmer" Steve, a "very shy and withdrawn invariably helpful (man) but with little interest in people or in the real world. A meek and tidy soul, he has a need for order and structure and a passion for detail" (Kahneman, 2013, pp. 6-7). To the natural question whether Steve is a farmer or librarian, most people would take the shortcut, considering occupational stereotypes would qualify him as a librarian. Nevertheless, careful contextual analysis indicates the ratio of male librarians to male farmers is so small, that the probability for Steve to be a librarian is only one in 20.

Case studies, such as that offered by Kahneman, must reveal hidden problems, because in this manner they will offer opportunities to take actions against further problems, as well as a better strategic understanding of the present and new research for the future.

As I mentioned, case studies ideally need to rely on data from several sources in order to be valuable lessons, but this also raises some legal and ethical questions, particularly for intelligence practitioners, who most times have first-hand knowledge on particular national security cases. Sharing too much in unclassified contexts would be a violation of legal provisions, while not saying anything, particularly in those situations where some measures are enforced in order to keep the secrecy, would be contrary to the rule of using multiple methods to collect data for case studying. And there is also the risk for the practitioner to ignore most publically available data due to inside knowledge.

In intelligence, case studies generally rely on intelligence successes or failures of the country`s own agencies or of reliable partners with similar responsibilities, but it is only the highly public ones which make it to the forefront.

Limitations in case studying

One of the most difficult questions I had to answer in my academic career was about whether specific events of the Romanian society in the former decade were actually failures of the Romanian intelligence. Student questions such as whether nosocomial infections

and the superficial manner of dealing with them in the Romanian public health system are easier to manage now, after extensive communications by the Parliamentary Oversight Committee, former decision-makers and the Service itself, but would have been much more difficult to answer under the normal **secrecy regulations** applying to most intelligence activities.

And a particularly difficult enterprise for Romanian intelligence studies is, with the Romanian intelligence field and agencies being still young – to bring to classrooms case-studies from our Romanian experience, not because there is a lack of such experience, but because it is, for the most, still classified.

As any other research instrument, case-studying must fulfil specific criteria of validity and reliability in order to be considered useful. Testing the validity of a case-study must be done through honest answers for two basic questions (Kumar, 2011, p. 178): 1) is it providing answers to the research questions; and 2) are the answers using appropriate methods and procedures?

And while case-studying in intelligence can be used both for quantitative and qualitative research, it is obviously more difficult to standardize data collection and to afterwards establish validity and reliability for qualitative research, since reliability means a consistency of the findings when situations repeat.

Validity of a research instrument can be measured, according to some researchers (Guba and Lincoln, 1994, pp. 105-117), based on four basic traits:

a. **Credibility**, meaning the results need to be believable for participants;

b. **Transferability**, that is the possibility to generalize results and transfer them to other, similar situations; this is a trait most difficult to establish in intelligence studies due to particularities pertaining to various fields; for example, it would be difficult to translate the American CIA actions into significant case-studies for the Romanian Intelligence Service (SRI), since the later is an internal security service and, as such, it needs to comply with very different criteria regarding the legality of its actions.

c. **Dependability**, meaning that observing similar events would lead to the same conclusions.

d. **Confirmability** or the corroboration of findings by others.

Intelligence failures from other states are among the most common case-studies we use in the classroom, because they are readily accessible and highly public affairs. But they are not always as relevant for the current intelligence situation in Romania, because the intelligence institutions are radically different in their missions, legislation, subordination and manner of cooperation.

For example, the most generally known recent intelligence failure is considered to be 9/11 and the American Intelligence Community`s inability to prevent it. First of all, the significance of the event and its quintessential case-study quality derives from the fact that it happened to the world`s greatest superpower and to some of the most famous intelligence agencies, if not the most powerful. The relevance of the case and its major impact stems from this very fact, while similar events – admittedly with fewer casualties – in countries such as Iraq or Afghanistan went practically unnoticed, despite hundreds of victims.

Nonetheless, there are fewer lessons intelligence students in Romania can draw from this dramatic event than one would initially think, due to several differences in the context; the general reason established by the Oversight committee in the US Congress as having led to the attacks was a lack of cooperation and information sharing among American security and intelligence institutions, a total of 16, whereas this would be rather difficult to replicate in the relatively small Romanian intelligence community, in which all actors have precise roles which do not often overlap.

There is also the thorny issue of the FBI headquarters failing to request a warrant for the informatics search of one of the attacker`s laptop, as exposed by FBI whistle-blower Coleen Rowley. She blames FBI organizational culture and hierarchy for this omission, since inexperienced headquarter officers were responsible for requesting warrants on behalf of regional offices. This is yet another significant difference from Romanian intelligence, which, on one side, has no law enforcement capacity, but for which procedures regarding national security warrants are different.

A significant reason for the deficit of knowledge which led to "9/11" was supposedly ignoring intelligence from foreign partners, which signalled suspect activities from the attackers. This is actually a universally valuable lesson in cooperation and information sharing with partners from all around the world.

Maybe one of the most worrisome conclusions of the "9/11" investigations in the US is the finding that not enough attention was paid by the CIA to adequate HUMINT, to providing the adequate resources. CIA had no assets within Al Qaeda before "9/11". While NSA was late to translate SIGINT intercepts of suspected terrorists, the overall American intelligence community had not enough knowledge about the Middle Eastern drivers and objectives. And this is yet another valuable lesson for any intelligence agency: the human (re)source is essential for progress, as are general resources for the national intelligence process.

But in retrospect, all things tend to seem easier and the perspective suddenly becomes much clearer once the pressure of time and imminent threat are off. And this, I think, is yet another limitation of case-studies.

Studying domestic cases can also prove difficult from more than one perspective. There is the obvious **need for secrecy** which greatly limits what can be discussed in public contexts. But there are also other types of impediments; for example, there are **strong public narratives** on some thorny issues, generated sometimes by the media or by involved/interested parties, but, in other instances, even by state authorities which, for political reasons, intentionally distort reality, reinterpreting an agency`s actions and even its fundamental missions.

In this case, given the difficulties of publicly presenting what is mostly classified information, many issues remain unanswered and impossible to case-studying. And there is also the problem of having to counter the official narrative, which, on one side, would undermine trust in public authorities, and on the other, would generate low morale among intelligence professionals, as well as a deficient organizational climate.

It is, nonetheless, important to the state that some initiative of case-studying past Romanian intelligence failures and successes was made by the Romanian Intelligence Service in its official *Monograph*

1990-2015 (2015) which, among others, describes controversial cases and operational successes throughout the institution`s evolution.

The case of the three Romanian journalists kidnapped in March 2005 in Baghdad and their safe return home was one of those relevant case-studies, able to illustrate perfectly the relevance of close **cooperation** among state institutions – in this particular case, SRI, External Intelligence Service (SIE) and Defence General Intelligence Directorate (DGIA), coordinated in their efforts by the establishment of an operative cell at the highest level in the state. This particular case was also a model of how close international cooperation and the good connections the Romanian intelligence had in the Middle East brought about extremely favourable results and saved human lives. Bringing the Romanian journalists back home safe was an intelligence success which amplified further cooperation with other foreign partners, in order to help solve similar cases.

Lack of adequate legislation, in Romania`s case, can also make it difficult to generalize common-sense conclusions from case-studying actions of other states. Terrorist online propaganda, for example, is one of those actions almost impossible to prosecute until very recently, since no Romanian law mentioned it as a national security threat or crime. Similar difficulties were specific to the past decades with regard to cyber-attacks and cybercrime, or even with legislation regarding the status of foreign citizens (which were, thus, difficult to expel or pronounce undesirable).

Other cases are, however, **universal lessons** in "how no to" practice intelligence. The Iraq invasion by the US is one such lesson, proving political involvement in intelligence and "**intelligence to please**" can lead to disastrous fails, such as claiming a country has nuclear arsenal only to prove, after military invasion with high costs for both parties, no such weapons exists.

Brief conclusions

Generalization is difficult for intelligence case-studies, due to different approaches at several levels, but a structured comparative analysis can, nonetheless, help identify some common traits.

I think it is a duty of honour for intelligence practitioners to have consistent in-depth analysis of their activity, and to honestly share their experience, in good faith and in observance of all rules and regulations governing the field.

Intelligence services, unfortunately, do not have the time and means to theorize, therefore making academia (both civil and military) a particularly adequate environment to further research and develop the field. And an academic environment such as the National Intelligence Academy or similar institutions attached to intelligence are real accomplishments because, on one side, they benefit from direct practitioners experience, and on the other, due to particular observance of the rules regarding access to classified information, help create a proper environment for in-depth analysis on sensitive topics.

Not only higher education institutions such as the "Mihai Viteazul" National Intelligence Academy are not obsolete, but they are an **objective necessity** for bringing together the **intelligence community, academia, similar partner institutions, and civil society**. This type of education centres have a significant and growing role, which brings added value to the intelligence activity in itself, but mostly to the overall state of security.

It is not, thus, a surprise to see the model of an intelligence academy was even promoted by French President Emmanuel Macron, in the form of an European Intelligence Academy, apt of "creating a shared intelligence culture among Member States" and responsible "for raising awareness among European and national institutions on intelligence issues".[2]

We need to benefit from all previous experience in order to prevent future failures. But it is also safe to understand that not all future events are preventable and not all past occurrences will serve as

[2] According to the official site of the French diplomacy, *Progress in European projects*, https://www.diplomatie.gouv.fr/en/french-foreign-policy/european-union/events/article/progress-in-european-projects-one-year-after-president-macron-s-initiative-for, accessed April 3rd, 2019.

valuable lessons. It is also essential to learn from others` experience, without having to suffer its bleak consequences.

References:

1. Budiansky, S., (2000), *Battle of Wits. The Complete Story of Codebreaking in World War II*, London, Penguin Books.

2. Chelcea, S., (2007), *Metodologia cercetării sociologice,* Editura Economică, Bucureşti.

3. Eriksson, J. & Giacomello, G., (2008), *Intelligence Studies and the Need for Theory: Strategic and Intellectual Challenges*, paper presented in the March 26-29, 2008 ISA Convention in San Francisco.

4. Guba, E. & Lincoln, Y, (1994), *The Handbook of Qualitative Research,* Sage Publications, Thousand Oaks, California.

5. Kahn, D., (September-October 2006), *The Rise of Intelligence* – Foreign Affairs, pp. 125-134.

6. Kahneman, D., (2013), *Thinking Fast and Slow,* Penguin Books.

7. Kent, S., (2019), *The Need for an Intelligence Literature,* on https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sherman-kent-and-the-board-of-national-estimates-collected-essays/2need.html, accessed April 3rd.

8. Kumar, R., (2011), *Research Methodology. A Step-by-Step Guide for Beginners*, Sage Publications, Los Angeles.

9. Johnson, L. (ed.), (2017), *The Handbook of Intelligence Studies,* Routledge.

10. *Monografia SRI 1990-2015*, RAO, Bucharest, 2015.

INTELLIGENCE AND CRISIS DECISION-MAKING: A BRIDGE TOO FAR?

Iulian CHIFU*

Abstract

Intelligence and decision making in crisis are intimately interconnected. Firstly, because of the beneficiaries of the intelligence activity (Davies, 2012), the decision makers. Secondly, because the acute need of suitable, in depth and accurate products (Hibbs—Pherson and Pherson, 2017), delivered timely is crucial in times of crisis. Therefore the interdisciplinary teaching, research and cross domains methodologies are crucial for the next generation of intelligence professionals who need to be closer to the needs of the beneficiaries, with a broader knowledge and a better capacity of communicating their analysis (Major, 2014). Our paper explores crisis decision making methodologies, prospective studies analysis, and scenario making instruments in order to provide a better focus and approach in intelligence teaching both in university and for specialization and training of the people already involved in the intelligence, when it comes the interaction between analysis and the beneficiaries.

Keywords*: crisis decision making, small groups' dynamics, prospective studies, intelligence briefers.*

Theory and practice, interference in intelligence studies. Early warning techniques. What to search for?

Intelligence studies should utilize the critical tools and techniques developed in related disciplines. The intelligence officers need to have solid methodological grounds for their assessments in order to reduce the number of errors, control them (Johnson, 2007), and know what the source of such errors of assessment is. Moreover,

* Associate professor at the National School for Political and Administrative Studies Bucharest and a professor at the National Defence University. He is the President of the Conflict Prevention and Early Warning Centre, Bucharest and a former advisor to the Romanian President in the fields of Strategic Affairs, Security and Foreign Policy.

knowing the methodologies of related sciences, time proved and with a lots of empirical feedback, helps also in knowing what to search for.

This is first and foremost valuable for an analysts, as long as the internal circuits of intelligence cycle allow at any point analysts to interfere with the process of data and intelligence gathering and communicating to operatives on the ground what they should look for in order to fill the gaps of the puzzle that analysts are trying to clarify and put together. As long as such a process of revision of data is ongoing inside the intelligence cycle, this type of knowledge is of tremendous interest, helping in raising the effectiveness and efficiency of the intelligence process (Hulsky and Schmitt, 2002).

There are specific fields where methodology is utmost importance for intelligence. The first is the whole spectrum of theories related to early warning. In fact, the very creation of an early warning system based on a complex of threats, risks, vulnerabilities is the best way of theoretically address intelligence gathering, intelligence analysis and effectiveness. It is also the way that any gathering intelligence plan is drafted (Hermann, 1999), followed by allocation of resources and building networks able to reach the targeted and needed data.

The knowledge of early warning tools and techniques, theoretical background and approach to mathematical control theories and approximation of errors is of tremendous importance in estimating the success and certainty of the results of an operation of intelligence gathering. It is also very important in order to know how big an error one can expect after such an endeavour (Jervis, 2010). It helps, on a distinct note, to avoid strategic surprises once we are talking about *black swan* events – low probability/high impact evolutions. Also it's useful for drafting any type of assistance from a computer model in that area, who needs to observe the rules of the theoretical models already identified.

For sure, intelligence has its own field of expertise and theories. Some are linked to psychology, to interpretation, some to the errors of small group decisions and groupthink. But relying on the theoretical ground already developed in other scientific domains helps a lot in narrowing errors of assessment and streamlining the search for valuable facts and data for intelligence products.

Conflict analysis. Need for effective prevention. Critical indicators

Another field of research and expertise with its own methodological background and methodologies is the conflict analysis, or as it has originally named, Conflict Resolution (Ramsbotham et.al. 2005). A well-established domain, a discipline well developed since 1965, where techniques of approaching it are based on solid grounds and more than half of century of research. It would be a pity to not use this field of research and its achievements.

The conflict analysis methodologies, from definition of concepts and Galtung's models, with the full debate about perception of self and of the other – in the Cain and Abel approach (Chifu and Lupu, 2016) – with the escalation/de-escalation model or the hourglass model are of tremendous importance for the number of experiences and analysis made based on those methodologies (Wallenstein, 2003) and the very careful evaluation of errors.

This helps when those models are applicable to any type of conflict (Deutsch et.al. 2006), either it is an inter-personal one, a community level, a societal conflict or even an interstate military one. The methodology helps in identifying the turning points and the stages achieved by which actor being analysed. And it helps create the charts for the critical indicators that to be followed in order to know the escalation model or, on the contrary, the turning points and the de-escalation path (Sandole et.al. 2009).

Knowledge is also well served when following the very subtle indicators that make the passage from dispute to contradiction, from an existing contradiction to conflictual attitudes of the two or more parties involved in a conflict and from the manifest attitudes to really acting aggressively, to a conflictual behaviour with its own stages of violence (Levinger, 2013). It also help since for each such stage, conflict analysis has drafted, exercised and applied tools and techniques in order to contain, to avoid escalation and to de-escalate the conflict, or to predict the re-ignition and explosion of violence (Jeong, 2008).

For an intelligence service it is of utmost importance that the strong theoretical base allows it to know what to look for, where to search for those critical indicators that make the difference between

war and peace (Hermann, 1999), between a domestic fight and a hate crime, and where to find hints on every evolution of such a developing conflict. This is a real challenge and nobody should deny this transfer of methodologies.

And here we are not talking about the very important studies developed in interethnic conflicts and religious conflicts (Said et.al. 2001), with their own instruments dealing with radicalization or inter-sectarian conflicts. Here psychology is playing an important role, as do studies related to the fundamental needs of and the individual, including identity, the individual and group identity (Chifu, 2012a). These needs, once they are not fulfilled, the individual is exposed to the offers to obtain a purpose in life, to find the true belief and to play a role, hold a position and deal with important tasks inside its community, a community that appreciates him. Those mechanisms are a clear path to radicalization and transitioning to action (Chifu, 2012b), from attitude to a radical behaviour and to terrorist action.

Another field where these methodologies could be used are in informational warfare (Chifu and Nantoi, 2016). It is also a process that involves a lot of recent methods derivation from marketing and channelling into micro-targeting at the level of the whole population, split into categories that need to be addressed differently, see the 32 categories of Cambridge Analytica (Chifu, 2017). When the influence moves from consumer preferences to political ones and when those technique address the will and options of a citizen who is supposed to vote, we are already in a domain where fundamental threats to security, decision making capacity and leadership choice is at stake and those techniques need to be addressed properly (Simons and Chifu, 2017), learned and used in order to have counter reactions, to protect the population through awareness and education, and to identify the critical indicators to be monitor in order to prevent a possible external involvement in such evolutions and public choices (Chifu, 2015).

Crisis decision making as a tool for intelligence officers. Where to look?

Another field of direct interest for intelligence studies is the crisis decision making. I would even say that it is of major importance

to know the cognitive – institutional approach to crisis, to know the methodology of analysing decision making in times of crisis and to know what drives the reactions – both good and bad – of a decision maker in times of crisis (Stern, 2001). This is helpful also due to the fact that it involves an average decision maker who could be a normal person with average professional skills, elected in a public position and required to react and to solve a crisis.

Here the knowledge targets the most important and intimate decision making skills, preferences, the psychological structure of a decision maker, the dynamics of his small decision making team, and the possibility to influence such a dynamic. Moving further, a crisis is a specific situation of stress and pressure which is exposing internal skills, professional experience, knowledge and character of a decision maker, some characteristics that are very important for estimating his reaction (Chifu and Ramberg, 2007). How much rationality and how much emotion or ambition lies behind the decision. How such a person could be framed by external actors and guided in order to take a required or bad decision.

Crisis decision making is a field that is close to the intelligence studies because the whole mechanism of intelligence is also responsible dealing with or preventing a crisis, reacting to pressure and public perceptions, assisting decision makers with the best advice possible and much needed information in order to deal with a crisis (De Keiser and Tames, 2008). And, in that respect, there are some parts where intelligence is playing a crucial role.

Separating information from noise is a crucial endeavour in times of crisis. Under pressure, a decision maker do not have time to properly select and make the best use of the data and information that comes in flows and to realize what is really important (Sundelius and Bach, 2015). In that particular situation, intelligence itself could help and assist with proper filters in order to select the repetitive useful data coming from witnesses in a crisis, and to identify the marginal data with a unique source which could change dramatically the situation if proved true, so it needs to be saved for further evaluation, even though that data is not in the mainstream flow of information.

A second moment where intelligence is of help is in the conflict of values. For sure, it is up to the designated decision maker to choose, when he has to deal with competitive fundamental values, because he's entitled and legally assigned to do so. But there's also a moment where intelligence could help and assist when consequence management is involved. In order to have a proper and accurate representation of its actions and decisions, as well as a realistic pressure level he is dealing with in a specific case, it is of first importance that the decision maker knows what the consequences (Boin et.al. 2008) of its decisions are.

Furthermore, crisis decision making methodologies are helping when dealing with crises in the intelligence field. An analyst knowing the way crises are evolving and how those crises trends are managed has the possibilities to identify the critical indicators that must be monitored and where an agent should look in order to find the concrete hints about the way a crisis evolves. The characteristics of a decision making team and psychological premises for a decision maker are of tremendous importance in trying to anticipate and build scenarios for the future evolution of a crisis or of an actor who is supposed to deal with a crisis.

Prospective studies and scenario making. Lessons learned adapted for intelligence studies

Another field of research and domain that intelligence needs to follow is prospective studies. Here, too, methodologies are developed and results are on the table with a whole abundance of experiences and lessons learned. In prospective studies the first step lies in the selection of critical indicators and the errors of the original assessment (Chifu, 2015a). Moreover, the evolution speed of a process could ruin the premises and assumptions regarding its evolution.

Here lies one of the most important, I would even say, crucial tasks of an intelligence service: avoiding strategic surprise (Chifu, 2015b). In some parts of the world strategic surprise – meaning that a decision maker is not warned in due time about the possibility that a major change happens in his field of responsibility – could lead to the resignation of the leader of the intelligence institution in question. It is

about the prestige, credibility and legitimacy of the intelligence institution itself. So that strategic surprise should be avoided.

And it's not always easy to do so, in a turbulent world, with tremendous changes, happening very fast, with leaders and decision makers that ignore logic, professional advices and rational choices in favour of ideological / emotional ones or those influenced by the will to obtain advantages and benefits from the crisis (Chifu and Nantoi, 2015). It is true, a crisis is a threat and an opportunity, but playing with fire and the apprentice wizard approach could lead to huge catastrophes. And examples are abundant in contemporary crisis decision making, when playing with a high risk leads to losing control and creating catastrophes – Rene Thom's theory.

It is the case of Jose Maria Aznar and the Atocha train station terrorist attack (Ray, 2004), before general elections that he was in the lead with his Popular Party in Spain, and when he tried to win more and chose to blame ETA Basque separatist movement and its socialist political competitors for this. Before the elections the reality was revealed, Al Qaeda was to blame and the Popular Party lost elections, Spanish army retreated from Afghanistan and from that moment on, Spain lost its position of a reliable ally and a country willing to invest in eradicating international terrorism.

A second well known case is that of Prime Minister David Cameron: in order to win elections, he promised to organize a referendum for Brexit, and then, in order to maximize his political position, he organised the referendum for exiting the EU, with a clear expectation that the result is going to consolidate his pro-European position inside the Conservative Party (Eline, 2019). And the result proved to be unexpected, he lost his job as prime minister and left Great Britain in a bad position. So playing with high risk decisions and using emotional or ideological arguments instead of professional and rational ones could lead to complicated outcomes.

In the related field of scenario development, there's also a lot to learn which can be used in intelligence studies and practice about the way this is developed. First, it is about identifying relative certainties, critical uncertainties and tipping points in an evolution in order to come up with a scenario (Chifu, 2014). Then it is about the selection of critical

indicators and drivers of a process or another that we are studying in its evolution. And third, it is about arranging scenarios in trends, those with discontinuities and last but not least, the black swan scenarios (Chifu and Bălăşoiu, 2018).

We have developed a Romanian model in that respect and applied it to several cases and several moments, identifying even the mistakes and errors when assessing scenarios related to an ongoing crisis. The lessons learned lead us to consider the *black swan* scenarios developed for each of the relative certainty evolutions. And it really helped us in the scenario making. The aim to avoid strategic surprise forced both scenario making processes, in prospective studies as well as the practice in intelligence, to include the scenarios – as improbable as they could be – that have important impact if they occur. And that is also an added value for intelligence studies as the experience and lessons learned from the process of identifying critical indicators that are channelling the evolution of an analysed process in one direction or another.

Intelligence and decision makers. A Bridge too far?

Last but not least, I think it is important to include a lesson from the methodological added value that other fields and domain of scientific research could bring in the study and practice of intelligence. It is the case when analysts and decision makers in intelligence agencies have the knowledge coming from those related fields of scientific research and the specialists in those fields inside the agency.

It is as important as having an "integrator" of the scientific studies and related fields that could both "translate" and integrate inside the agency the results of the research in those fields or even know what to require from research institutions outside of the Agency that could help the intelligence institution in bringing in the needed theoretical and methodological help from the scientific community, with a due consideration of the limits that the interference of those two fields, intelligence with its degree of secrecy or at least high level of discretion, and the science and academic community, far more open and who needs to breath and validate its results and findings and to communicate its achievements.

Intelligence agencies should become – if it is not already the case – contractors of research done in academic fields, to have a proper and effective instruments of integrating the result of the scientific research in the fields already underlined. And the perspective of having experts in all those fields and, in any case, analysts that know well the resources they could get from those related fields of research and methodological approaches, is of first importance.

Coming back to the original problem of the relation between decision maker and intelligence agency, the magnitude of issues connected to that relationship is huge. Beginning with building trust in a reciprocal manner and respect for the other's attributes and position, continuing with avoiding suspicion about the interference in its own attributes and the independence of the decision maker, continuing with a good and fruitful communication in order to absorb the essence and content of the intelligence product, there are full range of issues that are creating a complicated agenda (Ekengren, and Simons, 2011).

It's not easy and the relationship between intelligence and decision makers can be, sometimes, a bridge too far.

Firstly because of the different culture – of secrecy, extreme rigour and professionalism as well as responsibility and normative accountability, on one side, and of working with perceptions, public trust and public communication (Olson, 2008), political approaches and vindication as well as power politics and accumulating relevance, on the other side – the level of understanding, suspicion and trust could be difficult to match.

Secondly, because there's also the public perception, amplified by the media, that intelligence services are trying to use or distort or even control the options of the decision maker (Svedin, 2011). For a political elected figure that's a second way of life and it will always run away from the perspective of being controlled or of not being in power and dominating the intelligence agency. It's a second nature and it plays in the hands of those who support the deepening of a rift between intelligence and decision makers.

Once trust is established and the parties know exactly what they want and are open for the cooperation, some other level of issues appears. First it is about understanding the role and attributes: some

decision makers would not take no for an answer and could not understand the limits of intelligence activity, in terms of time and capabilities. In other cases the decision makers could look suspiciously at the field of operations that an intelligence agency runs in other to fulfil their role.

The professional background of the decision maker can vary a lot in a democracy. He could have education or not, he could have a higher knowledge level or a lower one, he could have a capacity to learn fast or be slow. And Intelligence agencies need to work with all those kinds of decision makers (Boin, 2005). They must communicate with them, and let them know what they are doing to assist them, what they can do, and what is not under their immediate reach.

Papers, documents and intelligence notes are playing an essential role in communication. But sometimes this should be doubled with intelligence briefers and visual demonstrations, information and other new forms of making sense in a specific manner adapted to the decision maker in question (Major, 2014). And for that purpose it is a pressing need to know the character, professional background and level of knowledge as well as the preferences of the decision maker in question (Osborne, 2017).

In some cases the appetite for intelligence is naturally high. Curiosity, a level of knowledge of the field he is responsible for and the professional and individual skills are playing the major role. But in other cases the appetite is very limited and even ideological or personal experiences are preventing the decision maker from listening, absorbing and making the best use of the intelligence he receives (Hansen, 2007).

Here a pro-active approach is needed to capture the attention and skilful intelligence agency leaders, head analysts and intelligence briefers are entitled to use creative instruments in order to obtain a reaction from the decision maker which reveals what he is interested in and what he needs to know, how to draw his attention to a particular process that he needs to be familiar with in his job, and how to fill the gap between the cultures that are governing intelligence and political activities or administrative decision making (*Bengt and Hansen, 2007*). And that's a challenge that could mean building the necessary specific

bridges rather than abandoning a decision maker who does not understand the usefulness and benefits of the intelligence activity and how to use the products that he receives.

References:

1. Boin, Arjen, t'Hart, Paul, Stern, Eric, Sundelius, Bengt, (2005), *The Politics of Crisis Management. Public Leadership under Pressure*, Cambridge University Press.

2. Boin, Arjen, McConnell, Allan, Hart, Paul, (2008), *Governing After Crisis. The Politics of Investigation, Accountability and Learning*, Cambridge University Press.

3. Chifu, Iulian, (2004), *Analiză de conflict*, Ed. Politeia-SNSPA, Bucureşti.

4. Chifu, Iulian, Ramberg, Britta, (2007), *Crisis management in Transitional Societies*, CRISMART SNDC, Stokholm.

5. Chifu, Iulian, (2012a), "Conflicts, Conflicts of Identity. Religious Conflicts. Characteristics and Specificities", in Chifu, Iulian, Popescu, Oana, Nedea, Bogdan, *Religion and Conflict radicalization and violence in the Wider Black Sea Region*, Ed. Institutului de Ştiinţe Politice şi Relaţii Internaţionale, Bucureşti.

6. Chifu, Iulian, (2012b), "Religion and Conflict: Radicalization and Violence in the North Caucasus", in *Turkish Policy Quarterly*, Vol. 10, No. 3, Istanbul, pp. 121 – 132.

7. Chifu, Iulian, (2014), *Prospectives on Ukraine Crisis. Scenarios for a mid-long term evolution*, Ed. Institutului de Ştiinţe Politice şi Relaţii Internaţionale al Academiei Române, Bucureşti.

8. Chifu, Iulian, (2015a), "Prospective studies: a Romanian Metodology. Ukraine as a case study in Scenarios for a Short-Mid-Long Term Evolution" in "New Approaches in Social and Humanistic Sciences", 11-13 September 2015, Chişinău, Republica Moldova, Working Papers, International Conference, 16-19 April 2015, Iaşi, Lumen Media Publishing UK, 2016, ISBN 978-1-910129-05-0(ISI Thomson), pp. 75.

9. Chifu, Iulian, (2015b), *Prospective Analysis of Ukrainian Crisis: Scenarios for mid-long term evolution*, Ukraine Analytica, Nr.1/9 October 2015, Odessa.

10. Chifu, Iulian, Nantoi, Oazu, Getmanchuk, Aliona, (2015), *Prospective on Ukraine Crisis. A trilateral approach*, Ed. Institutului de Ştiinţe

Politice şi Relaţii Internaţionale "Ion I. C. Brătianu" al Academiei Române, Bucureşti.

11. Chifu, Iulian, (2015c), *Război hibrid, lawfare, război informaţional. Războaiele viitorului*, in Universitatea Naţională de Apărare, *Strategii XXI. Complexitatea şi dinamismul mediului internaţional de securitate*, Editura UNAp "Carol I".

12. Chifu, Iulian, Nantoi, Oazu, (2016), *Război informaţional: tipizarea agresiunii informaţionale a Federaţiei Ruse*, Ed. Institutului de Ştiinţe Politice şi Relaţii Internaţionale "Ion I. C. Brătianu" al Academiei Române, Bucureşti.

13. Chifu, Iulian, Lupu, Lavinia, (2016), *Analiză de conflict*, Ed. RAO.

14. Chifu, Iulian, (2017), *Trei generaţii de război informaţional. Nivelul dezvoltării domeniului în partea sa publică,* Revista Infosfera, Septembrie.

15. Chifu, Iulian, Bălăşoiu, Narciz, (2018), *Prospective studies of the Wider Black Sea Region. Scenarios for its future in times of high international turbulence*., Ed. Institutului de Ştiinţe Politice şi Relaţii Internaţionale "Ion I. C. Brătianu" al Academiei Române, Bucureşti.

16. De Keiser, Madelon, Tames, Ismee, (2008), *Small Nations. Crisis and Confrontation in the 20-th Century*, Walburg Pers.

17. Davies, Philip H.J., (2012), *Intelligence and Government in Britain and the United States*, Praeger, Santa Barbara, California.

18. Deutsch, Morton, Coleman, Peter T, Marcus, Eric C., (2006), *The Handbook of Conflict Resolution. Theory and Practice.* Second Edition, Jossey-Bass.

19. Ekengren, Magnus, Simons, Greg, (2011), *The Politics of Security Sector Reform. Challenges and Opportunities for the European Union's Global Role*, Ashgate.

20. Eline Schaart, (16.01.2019), *David Camron: "I don't regret calling Brexit Referendum"*, Politico, retrieved at https://www.politico.eu/article/david-cameron-i-dont-regret-calling-brexit-referendum/.

21. Hansen, Dan, (2007), *Crisis and Perspectives on Policy Change*, National Defense College.

22. Hermann, Michael, (1999), *Intelligence Power in Peace and War*, Cambridge University Press, Royal Institute of International Affairs.

23. Hibbs—Pherson, Katherine, Pherson, Randolph H, (2017), *Critical Thinking for Strategic Intelligence*, Second Edition, Sage, Thousand Oaks, California.

24. Hulsky, Abram N., Schmitt, Gary J., (2002), *Silent Warfare. Understanding the World of Intelligence*, Third Edition, Potomac Books Washington DC.

25. Levinger, Matthew, (2013), *Conflict Analysis. Understanding Causes, Unloking Solutions*, US Institute of Peace Press, Washington DC.

26. Jeong, Ho-Won, (2008), *Understanding Conflict and Conflict Analysis*, Sage Publications.

27. Jervis, Robert, (2010), *Why Intelligence Fails. Lessons from the Iranian Revolution and the Iraq War*, Cornell University Press, Ithaca and London.

28. Johnson, Loch K., (2007), *Handbook of Intelligence Studies*, Routledge, New York.

29. Major, James S., (2014), *Communicating with Intelligence. Writing and Briefing for National Security*, Rowman and Littlefield, London.

30. Olson, Eva Karin, (2008), *Media Crisis decision-making*, Stockholms Universitet.

31. Osborne, Gerry, (2017), *Strategic Communications. Practical Advice for Strategic Leaders*, M&C Saatchi World Services, NATO-Georgia.

32. Ramsbotham, Oliver, Woodhouse, Tom, Miall, Hugh, (2005), *Contemporary Conflict Resolution*, Second Edition, Polity Press, Cambridge, UK.

33. Ray, Michael, (2004), *Madrid Train Bombings of 2004*, Encyclopaedia Britannica, at https://www.britannica.com/event/Madrid-train-bombings-of-2004.

34. Said, Aziz Abdul, Funk, C. Nathan, Kadayifci, Ayse, F., (2001), *Peace and Conflict Resolution in Islam. Precept and Practice*, University Press of America.

35. Sandole, Dennis J.D., Byrne, Sean, Sandole-Staroste, Ingrid, Senehi, Jessica, (2009), *Hanbook of Conflict Analysis and Resolution*, Routledge.

36. Simons, Greg, Chifu, Iulian, (2017), *The Changing Face of Warfare in the 21st Century*, Ed. Routledge, London and New York.

37. Stern, Eric K., (2001), *Crisis Decisionmaking. A Cognitive-Institutional Approach*, CRISMART, Stockholm.

38. Sundelius, Bengt, Hansen, Dan, (2007), *Crisis and Perspectives on Policy Change. Swedish Counterterrorism Policymaking*, CRISMART, Stockholm.

39. Sundelius, Bengt, Bach, Robert, (2015), *Strategies for Supporting Community Resilience. Multinational Experiences*, CRISMART, Stockholm.

40. Svedin, Lina, (2011), *Ethics and Crisis Management*, Information Age Publishing.

41. Wallenstein, Peter, (2003), *Understanding Conflict Resolution. War, Peace and the Global System*, Sage publications.

HISTORY AND MEMORY IN INTELLIGENCE

USING HISTORY AS A TOOL IN INTELLIGENCE EDUCATION

Lars BAERENTZEN*

Abstract

Using historical events as training material is, I think, more illuminating than using constructed scenarios because history often includes elements that the author of a scenario must reject as being impossible or too unlikely. However, as a tool for understanding current affairs both for the politician and for the intelligence analyst, history has a right use and a wrong use. Therefore so many people believe "that the only thing one can learn from history is that one cannot learn anything from history"? In this respect I will try to answer the following question: How useful is historical knowledge and training as an historian for an intelligence analyst?

Keywords: *history, intelligence, education, useful tool for teaching.*

Introduction

Konrad Adenauer wrote at the beginning of his Memoirs (for 1945-1953) that he had recently asked a German Professor of Modern History how he, as an historian, believed the future would be. The professor said that historians are not prophets. Adenauer replied "I believe that historians, and especially a professor of modern history, must at least make an attempt, through analogies based on what has happened in our time, even in recent days, to understand in what direction developments are likely to go, and they must in their teaching say what developments should be expected and possibly warn about them." (Adenauer, 1965) The professor did not agree with Adenauer.[1]

---

* Historian and a former intelligence practitioner for Danish Defense, independent consultant and lecturer.

[1] "Vor kurzem unterhielt ich mich mit einem Historiker, Professor für neuere Geschichte an einer deutschen Universität, über unsere Zeit. Im Laufe des Gespräches fragte ich ihn, wie er als Historiker sich die Entwicklung denke. Er antwortete mir, es

How useful is historical knowledge and training as an historian for an intelligence analyst?

It is very useful indeed, in my view. But if this is true, then why do so many people believe "that the only thing one can learn from history is that one cannot learn anything from history"? Because, as a tool for understanding current affairs, history has a right use and a wrong one both for the politician and for the intelligence analyst. The *wrong use* is to look for parallels in history to what is happening just now and then expect a similar outcome of the current situation. Parallels will only be parallels, situations are never the same, and the outcome of today's crisis can easily be the opposite of what happened in the past. The *right use* is for the politician or the analyst to use historical knowledge as a constant reminder how humans have acted in similar situations in the past, of how often plans and expectations turned out to be different from what *actually* happened – but also as a reminder of modes of action or behaviour that worked as intended and created the results which the actors aimed for.

I think this is what Thucydides meant when he wrote that he would like his book to be useful to future readers who would want to understand events happening to themselves that were "like or similar to" the events he had described.[2] Of course, if historical knowledge is

---

sei nicht Aufgabe des Historikers, Entwicklungen im voraus zu sehen. Die Historiker seien eben keine Propheten. Ihre Aufgabe sei es, das, was geschehen sei, möglichst wahrheitsgetreu festzuhalten oder zu ermitteln. Ich erwiderte ihm, ich hätte von der Aufgabe eines Historikers eine andere Meinung. Ich sei der Auffassung, die Historiker, namentlich ein Professor der neueren Geschichte, müssten wenigstens den Versuch machen, auf dem Wege von Analogieschlüssen aus dem Geschehen unserer Zeit, sogar unserer Tage, zu erkennen, wohin der Lauf der Entwicklung wahrscheinlich gehen werde, und sie müssten in ihrer Lehre hinweisen auf zu erwartende Entwicklungen und eventuell warnen. Der Historiker gab mich nicht recht. Er wiederholte nochmals, Historiker seien keine Propheten. Ich verlange natürlich keine Prophezeiungen von einem Historiker, aber ich meine, seine Arbeit, namentlich bei einem Historiker für neuere Geschichte, sei nur wirklich getan, wen er, so gut wie möglich, zukünftige Entwicklungen aus dem jetzigen Geschehen folgere." Konrad Adenauer: Erinnerungen 1945-1953, 1965, p. 13. My translation (abridged).

[2] Thucydides: The Peloponnesian War, I, 22: καὶ ἐς μὲν ἀκρόασιν ἴσως τὸ μὴ μυθῶδες αὐτῶν ἀτερπέστερον φανεῖται: ὅσοι δὲβουλήσονται τῶν τε γενομένων τὸ σαφὲς σκοπ

to be useful in this sense, it must reflect an honest attempt to look at the past.

Using historical "parallels" that are just propaganda is worse than knowing no history at all. The following is a good example of using history badly: "In 2004, when the expansion of NATO towards the East was big news, a Texas newspaper published a triumphalist account of Poland's NATO accession, under a photo of Polish soldiers and the headline "No more Yaltas, No more Munichs". "Yalta" and "Munich" are here reduced to catchwords meant to add historical prestige to the idea that giving in to force" is wrong and humiliating." But no more examples of how *not* to use history.

Now a good example for the positive way: The study of history gives the analyst a wide knowledge of what *can happen* and *may happen* in human affairs[3] and teaches him or her that:

εῖν καὶ τῶνμελλόντων ποτὲ αὖθις κατὰ τὸάνθρώπινον τοιούτων καὶ παραπλησίων ἔσ εθαι, ὠφέλιμα κρίνειν αὐτὰ ἀρκούντως ἔξει. κτῆμά τε ές αἰεὶ μᾶλλον ἢ ἀγώνισμα ές τὸ παραχρῆμα ἀκούειν ξύγκειται. (Translation of the author): "And perhaps my history will seem less amusing to listen to because of the absence of good stories. It will be enough for me, however, if this work of mine will be judged useful by those who will want to understand clearly the events which happened in the past and those which (in accordance with human nature) will probably happen in the same or similar ways in the future. My book is a possession for eternity rather than something to attract immediate admiration. Among the vast number of comments on the meaning of this passage perhaps that made by A.W. Gomme is most useful: "It should not be necessary, but it is, to explain that will probably happen… in the future is future to Thucydides, not to his readers: the latter will not find his work useful in order to divine what will happen in the future, as though it were a sort of horoscope, but for the understanding of other events besides the Peloponnesian war, future to Thucydides, but past or contemporary to the reader … That is why it is to be a possession for eternity> and the events of the last twenty-five years in Europe only prove that Thucydides' hopes for his History were to be fulfilled much more completely than even he ever expected." A.W. Gomme, *An Historical Commentary on Thucydides*, vol I, p. 149, Oxford 1956 (first published 1944).

[3] The historian J.C. Masterman (who was secretary of the "XX Committee" during the Second World War, which ran the "Double-Cross system") has written on the value of history in general: "For ordinary men and women the prime value of the study of history is that it vastly enlarges human experience. The true student forms his judgements, not upon the few and uncertain precedents of his lifetime, but upon the accumulated experience of the past. He learns the all-important habit of discriminating between the important and the trivial; he establishes for himself a true

- the result of a plan or an action is rarely (if ever) *exactly* what was expected by those who launched the initiative.
- the careful planning and preparations increase the odds for success, but offer no guarantee for it;
- the factors which seem distant and irrelevant to the issue at hand may yet have decisive influence on the outcome.

Using historical events as training material is, I think, more illuminating than using constructed scenarios because history often includes elements that the author of a scenario must reject as being impossible or too unlikely.[4]

Also, in history, the analyst benefits from learning how military and political actions have often been based on considerations or information (for instance from intelligence) known to very few people when they happened. The history of The Second World War is filled with such examples which have only become available to historians decades after the war ended. Indeed, for thirty years after 1945 the British Government prevented historians – including the "official historians" – from telling the truth about the most important achievements of British intelligence. Generals and politicians in their memoirs had to attribute important decisions to their own foresight or wisdom, and to hide knowledge derived from code-breaking.[5] (Some did not seem to mind that).

---

standard of values; he is not to be stampeded into magnifying unfortunate episodes into catastrophes. In short he gains judgement and balance and wisdom, all based not on the brief experience of a single lifetime but on the truths culled from many generations. If this is true of the study of history, how much more is it true of that of Universal history? And what task could be finer or nobler than that of the Universal Historian?" (Masterman, 1961, p. 83)

[4] I venture this observation based on 25 years of experience of designing "crisis management games".

[5] On 31 July 1945, the Joint Intelligence Committee approved a general directive to heads of the Official History programs that the existence of such intelligence <meaning: Ultra and Bletchley Park> "should NEVER be disclosed". Historians on their staffs who were not privy to the Ultra secret should be instructed "not to probe too deeply into the reasons for apparently unaccountable orders being issued". The underlying justifications for secrecy were twofold: first, and more obvious, not to arouse the suspicions of future enemies about British skill in signals decryption, which would encourage them to take countermeasures. Second, and more interesting, was

The First World War is also of great use for training future intelligence analysts because of the historical disagreements about many fundamental issues which are still vivid and unresolved now, a hundred years later, after generations of historians have studied them. If a particular great event has been studied by many authors over a long time, details are known that could not have been known to contemporary observers, again a useful lesson to an analyst.[6] *What* history, then, should be included in a curriculum presented to the coming intelligence analyst? Ideally, *the whole history*! Since this is not possible, I will now present a sketch of five lectures, each under a headline indicating what specific "mode of thinking" which that history lecture will, I hope, teach the student of intelligence analysis.

History lessons for intelligence analysts

History on a grand scale: The analyst should know about the Rise and Fall of the Roman Empire, about the Ottoman expansion to the walls of Vienna and the subsequent contraction, about the Thirty-Years' war, about the wars of the French Revolution, about the first and second World Wars of the 20th century, and about the Cold War. He or she must know that when the Mongols were overrunning Europe in 1241, the Europeans were only saved because the great Khan suddenly died and the attack was called off. Moreover, when King Frederick the

the fear that if the Germans and Japanese became aware of the part played by special intelligence, they might claim they had not been fairly defeated – an echo of the "stab in the back" myth about the German collapse in 1918. ... These arguments justified a major program of censorship. The official histories of the war carefully concealed all traces of Ultra, becoming what has been called "the last deception operation of the Second World War," and would-be memoir writers in the know were pressured to keep silence. Remarkably, it was not until 1974 that the wartime Head of Air Intelligence, Frederick Winterbotham, with reluctant official approval, published his personal account, *The Ultra Secret* in David Reynolds: In Command of History. Churchill fighting and writing the Second World War, New York, 2005, p. 161-2.

[6] My use of old historical examples is open to this critical question (posed by my friend Lt.Col. L.T. Larsen): *It is all very well for understanding the world we knew! But how can they relate to modern issues like e.g. Cyber Warfare? How can history illuminate a type of war that as yet has no history?* I think the question is natural, but that it is not valid: The teaching of history deals with the way humans behave in conflict, not with the specific tools or methods of war.

Great of Prussia was being crushed by his enemies in 1762, the Russian Tsarina died suddenly – and Prussia was saved. When Hitler in 1945 believed that he and the remnants of Germany could be saved by similar luck, Roosevelt in fact died on April 12, 1945, but Nazi Germany was not saved from its enemies.

He or she must know how European statesmen feared a general war sparked by the Balkan wars of 1912-13; how that war was avoided, but broke out in 1914 after the murders in Sarajevo. How leaders and peoples in all the warring states in 1914 expected a short war leading to decisive results and how the war instead dragged on and on – and created a new world order with Europe in a less central role.

Everyone will draw their own conclusions from studying history on a grand scale.[7] Some may agree with Lloyd George who summed up his view of World War One in these words: *"Chance is the supreme judge in war and not Right. There are other judges on the bench but Chance presides. If Germany had been led by Bismarck and Moltke instead of by von Bethmann-Hollweg and Falkenhayn, the event of the great struggle between a military autocracy and democracy would in all human probability have been different. The blunders of Germany saved us from the consequences of our own. But let all who trust justice to the arbitrement of war bear in mind that the issue may depend less on the righteousness of the cause than on the cunning and craft of the contestants. It is the teaching of history, and this war enforces the lesson. And the cost is prohibitive. It cripples all the litigants."* (Lloyd George, 1936, p. xv)

History that teaches to expect the unexpected: In mid-January 1991, when Iraqi forces were still entrenched in Kuwait, but an attack by the forces under American command poised in Saudi-Arabia to drive the Iraqi army out could be expected any moment, intelligence observers were generally in agreement that the smart thing for Saddam Hussein to do would be to withdraw his forces voluntarily – or just to begin doing so – or just to say that he intended to begin withdrawing

[7] Obviously these short paragraphs represent my own interpretation and understanding of these complex historical events.

them.[8] It seemed obvious that an Allied attack would not, in that case, have been politically possible. But Saddam did not act as many observers expected. History often demonstrates that what one side expects the opponent to do is not what he does. The German attack in November 1944 through the Ardennes was a surprise that proved very costly to the Allies, especially to the Americans.

Moreover, Stalin had certainly been warned by the British, the Americans and by the Swedes about the German operation Barbarossa on June 22, 1941, but he chose to think – apparently – that the warnings were "provocations" intended to involve Russia in war with Germany.[9]

In August and September 1944 there were frequent secret contacts or "feelers" between the British and German enemies in occupied Greece. Some very high-ranking German officers (among them Field-Marshal von Weichs and the German political chief in the Balkans, Neubacher) saw these clandestine contacts as a chance to come to an "understanding" with the British against the Russians. In the German military headquarters, this was the miracle that nearly everyone was hoping for. The idea was presented to Hitler and in September he vetoed any further contact. Why? No one knows – ? (Bærentzen, 1980, pp. 23-62)

In History, the list of surprises is perhaps without end. In more recent times, American intelligence in the late 1970s knew very well that the Shah of Iran was under pressure from religious Iranian leaders, and it was also known that a certain Ayatollah named Khomeini, in exile in Iraq, was a source of much worry and even fear in the ranks of the Shah's own secret police. However, US analysts remained convinced

[8] This statement is based on the author's personal recollection.

[9] For example, the British Government on 11 June 1941 told Russia in detail about the German military preparations against the Soviet Union. But Stalin disbelieved this and many other warnings: "Stalin's chief GRU (military) adviser, F.I. Golikov, the officer personally responsible for passing the bulk of the intelligence to him – as Menzies was to Churchill – was as a survivor of the purges all too aware of Stalin's pathological paranoia. Reports that confirmed his master's suspicions he carefully classified as 'reliable'; the others he described as 'doubtful'. And while punctiliously passing to Stalin the German operational plan for Barbarossa, he noted that it was 'merely the work of agents provocateurs aiming to embroil Germany and the Soviet Union in war'." David Stafford: Churchill and Secret Service. London, 1997, p. 222.

that the Shah's pro-western regime was secure, almost to the day it fell. President Carter's national security adviser, Zbigniew Brzezinsky, wrote in his memoirs that he was sorry he had not engineered a coup in time to stop Khomeini.[10]

The historian has the luxury of being able to admit that something quite unexpected did happen, and he may then proceed to explain why this was, surprisingly, what took place. Sometimes, but not always, the reasons become clear in hindsight. It takes a brave intelligence analyst to maintain that the unlikely is what will happen.

History of intelligence successes and failures: Some intelligence successes achieved in the Second World War which can now be studied are fantastic. For example, the ability of the British and the Americans to read the encrypted messages of their enemies surely had an impact on the course of the war. The ability, in addition, to make use of the deciphered information in military operations disguised in such a way that the Germans never realized that their communications were compromised was an equally remarkable success. Knowing what the enemy believes and what orders he sends out enabled the British to build up a series of deception schemes. The most famous was surely "Operation Fortitude" intended to convince the Germans that the invasion in Normandy on June 6, 1944, was only a forerunner to a larger invasion that would soon after land at Calais. (Hesketh, 2002) The "German agent" who convinced the Germans of this deception received a German decoration, although he was in fact a Spaniard working for the British. His codename was *Garbo*. (Harris, 2000)

[10] "Perhaps that disaster <the fall of the Shah> was historically inevitable, the Islamic fundamentalist wave too overpowering, and perhaps the Shah could never have been saved from either his own megalomania or, in the end, his paralysis of will. But my pained belief is that more could have been done by us on the American side. Historical determinism is only true after the fact." Zbigniew Brzezinski: Power and Principle, p. 354. Later in the book, Brzezinsky quoted his own diary for 20 February 1979 for this statement about Iran: "A depressing story of chaos and confusion. The more I hear of what is going on, the more depressed I am over the fact that I did not succeed in getting the U.S. Government to approve and, if necessary, to initiate an Iranian military coup." Zbigniew Brzezinski: Power and Principle, p. 393.

The historian can easily be dazzled by these successes and naturally analysts must learn about them during their education. The wealth of secrets now open must not, however, overshadow the fact that not all the secrets of the Second World War have yet been disclosed. One example: Which side deceived the other during the so-called "*Englandspiel*" in 1942-43? (Wolters, 2003)

The successes are fascinating, but it is more useful for analysts to study the reasons that led the enemy to be fooled or taken in. Why did the German side continue to believe that their encrypted messages were safe – in spite of many episodes that could – and perhaps should – have alerted them to discover the truth? In my view, the many reasons which in the aggregate led some very competent German cryptology experts to believe in the security of their communications are easy to understand – and they are probably similar to factors that today's analysts need to worry about.

Why did the U.S. Government for a long time believe in the existence of Iraqi weapons of mass destruction and continue to use some false information as part of the justification for the attack against Saddam Hussein in 2003 – in spite of the fact that doubts about the credibility of its source (known by the codename *Curveball*) should have made them more careful? Today, almost twenty years later, there is a great debate about the whole issue. Perhaps we are too close in time to call it "history", but its study will undoubtedly benefit future analysts.

Back to World War II: Sometimes one and the same event is an intelligence success but a military disaster. Before the German parachutists attacked the British forces which had fled to Crete from mainland Greece, the codebreakers at Bletchley Park had produced almost complete information about the German attack plan. Even more notable, this information was in the hands of the British commander on the island, the New Zealand General Freyberg, who remarked, when the German planes appeared on the horizon: "They are on

time".[11]Moreover, in spite of the fantastic intelligence the British lost Crete and were evacuated to Egypt. This episode of the war brings to mind the historian John Keegan who ended his book on "Intelligence in War" with this warning: *Knowledge of what the enemy can do and of what he intends is never enough to ensure security, unless there are also the power and the will to resist and preferably to forestall him. .... Foreknowledge is no protection against disaster. Even real-time intelligence is never real enough. Only force finally counts.* [12]

How the Balkans was divided one evening in Moscow: It is now a famous story – Churchill and Stalin met in Moscow on October 9, 1944, and agreed about their respective spheres of influence in the Balkans. It is about the so-called "Percentages Agreement", because Britain's and Russia's respective degree of influence in each Balkan country was expressed as a "percentage". What did the percentages mean? No one knew precisely.[13] Nevertheless, the military and political events in the Balkans during the rest of the war, and the subsequent partition of the whole area during the Cold War, took place in near perfect agreement with this "scrap of paper". Britain, and later the U.S., had a "free hand" in Greece: Stalin did not interfere with their defeat of the Greek communists, similarly the Western Allies did not try to prevent Russia from doing what she wanted in Romania. Indeed, Stalin's blue tick on the paper was placed precisely over the word "Romania", *perhaps* indicating that here was his principal interest.

It took a long time before the existence of this "agreement" became known outside a very narrow circle. Its effect, however, was

---

[11] Freyberg's remark was heard by a British officer who was nearby: "Shortly after dawn on 20 May I had to take a message to Freyberg at his headquarters in Khania (Canea): why, or what about, I cannot recall. He invited me to stay for breakfast on the veranda of his villa. The sky was exquisitely blue – a perfect early summer day; but momentarily looking up, I was startled to see the sky full of gliders and parachutists. Freyberg did not let it spoil his breakfast. He looked up, grunted, and remarked: 'Well, they're on time!'". (Woodhouse, 1982, p. 13)

[12] John Keegan: *Intelligence in War. Knowledge of the Enemy from Napoleon to al-Qaeda. New York*, 2003, p. 348-349.

[13] Churchill's account of this meeting was published in 1954 in vol. VI of his The Second World War, p. 197-98.

soon visible on the ground. The Soviet military attaché in Athens, Col. Popov, stayed in his room in the Grande Bretagne Hotel, reading, or in the bar, drinking, while British forces in Athens were fighting and defeating the Greek partisans in the streets around the hotel. Churchill and his government were violently criticized, *but in the House of Commons and not by Stalin*, for making war again the Greek guerrilla fighters, "who had so recently fought against the Germans".

Can it be of any use to intelligence analysts in a later age to know about an historical episode that is so obviously tied to a particular time and place, dependent on a unique set of circumstances, and enacted by two unusual actors (to put it mildly): Churchill and Stalin? No, of course not, or not directly! But knowing about those "percentages" might inspire ideas about how to understand situations where the visible actors seem to act quite differently from what one would expect them to.

It is, of course, a basic condition of intelligence analysis that not all the relevant facts are known to the analyst. The object of his or her understanding is often a moving target. Both the actions and the words that have to be interpreted and understood may change with no warning. Both the historian and the analyst experience gaps in the knowledge which they would want to have, but with important differences. The historian may spend years writing a book or an article and look for new sources at leisure. The analyst is often under pressure of time, but, on the other hand, the analyst may sometimes ask for, or even instigate, the interception of new sources.

Two examples of this latter practice are well known, the first one is even famous. When U.S. intelligence in May 1942 believed, but were not sure, that the two letters "AF" in Japanese decrypted signals meant "Midway", they engineered the sending of an unencrypted signal from Midway saying that their fresh water machine had broken down – and soon after, a Japanese signal reported that "AF is short of fresh water".(Kahn, 1996, p. 569) Moreover, British codebreakers found that German signals about Allied mine-laying could be used as an important tool for breaking new Enigma settings – so aircraft were sometimes sent out to lay mines for the sole purpose of inducing the sending of these useful signals. (Noskwith, 1993, p. 122)

How should history be taught to intelligence analysts?

A source of inspiration for the teaching of history to students who are going to be intelligence analysts is the way work is done by those committees charged with investigation of accidents. Whether they are single events with many victims (in the air) or frequent, but smaller events (on the roads), the investigators make strenuous efforts to uncover and understand the causes. The causes are always complex and typically include factors like technical defects and local conditions at a particular accident and human factors like the physical and mental condition of the driver or the pilot.

The idea of comparing wars and road accidents is of course not my own. A.J.P. Taylor (1965, p. 135-136) put it in these words: *"Wars are much like road accidents. They have a general cause and particular causes at the same time. Every road accident is caused, in the last resort, by the invention of the internal combustion engine and by men's desire to get from one place to another. In this sense, the 'cure' for road accidents is to forbid motor-cars. But a motorist, charged with dangerous driving, would be ill-advised if he pleaded the existence of motor-cars as his sole defence. The police and the courts do not weigh profound causes. They seek a specific cause for each accident – error on the part of the driver; excessive speed; drunkenness; faulty brakes; bad road surface. So it is with wars. 'International anarchy' makes war possible; it does not make war certain."*

If a particular type of aircraft is suspected of being too risky to fly, it can be ordered to stay on the ground. If an intelligence analyst in a current crisis sees historical parallels that once led to catastrophe, he can only warn and try to dissuade from the course of action wanted by his boss, the statesman. Unlike the accident investigator who can sometimes enforce changes in rules or conditions that really prevent future accidents from happening, history and politics are more complicated and both leave margins of doubt that allow the actors of today to ignore the lessons of experience – if tempting gains speak for action anyway.

For example, on 28 February this year, 2019, a sudden and dangerous crisis erupted between India and Pakistan. Apparently that crisis was defused after the Prime Minister of Pakistan acted in a

conciliatory way, allowing a captured Indian pilot to go free, and on television he said: *"All wars are miscalculated, and no one knows where they lead to. World War I was supposed to end in weeks, it took six years. Similarly, the US never expected the war on terrorism to last 17 years".* Moreover, the crisis which began the Second World War was not defused, although Prime Minister Chamberlain in a letter to Hitler on August 23, 1939, used an historical argument: "*It has been alleged that, if His Majesty's Government had made their position more clear in 1914, the great catastrophe would have been avoided. Whether or not there is any force in that allegation, His Majesty's Government are resolved that on this occasion there shall be no such tragic misunderstanding."*[14]

Conclusion

So the historian must admit to his analyst students that although history as well as intelligence analysis may, in a specific situation, seem to warn of great danger, such warnings will never, or very rarely, prevent the statesman from going to war if he wants to do so. This pessimistic conclusion is probably true of any age, but risks are likely increased when rulers are particularly disrespectful of facts. In September 2016, Graham Allison and Niall Ferguson proposed that The White House needed a Council of Historical Advisers. They also suggested that the charter for this council *"begin with Thucydides's observation that "the events of future history … will be of the same nature — or nearly so — as the history of the past, so long as men are men."* (Graham and Ferguson, September 2016) As far as I know nothing has been heard about this idea since 2016.

[14] Miscellaneous no. 9 (1939) Documents concerning German-Polish Relations and the Outbreak of Hostilities between Great Britain and Germany on September 3, 1939. Presented by the Secretary of State for Foreign Affairs to Parliament by Command of His Majesty. London, 1939. Cmd. 6106. (Letter 56, p. 96-97)

References:

1. Adenauer, Konrad, (1965), Erinnerungen 1945-1953.
2. Bærentzen, Lars, (1980), *Anglo-German Negotiations during the German Retreat from Greece in 1944.* In: Scandinavian Studies in Modern Greek, no. 4, pp. 23-62.
3. Graham, Allison, Ferguson, Niall, (September 2016), *Why the U.S. President needs a Council of Historians*, The Atlantic.
4. Harris, Roger, (2000), *Garbo. The Spy who saved D-Day*. Introduction by Mark Seaman. Public Record Office Secret History Files. London.
5. Hesketh, Roger, (2002), *Fortitude. The D-Day Deception Campaign*. Introduction by Nigel West. Woodstock & New York.
6. Kahn, David, (1996), *The Codebreakers. The Story of Secret Writing*. Revised edition, New York.
7. Keegan, John, (2003), *Intelligence in War. Knowledge of the Enemy from Napoleon to al-Qaeda*. New York.
8. Lloyd, D. George, (1936), *War Memoirs*, vol. VI.
9. Masterman, J.C. (1961), *The Martyrdom of Man*, in: *Bits and Pieces*, London, 1961.
10. Miscellaneous no. 9 (1939) London, 1939. Cmd. 6106. (Letter 56, p. 96-97)
11. Noskwith, Ralf, (1993), *Hut 8 and naval Enigma*, in F.H. Hinsley and Alan Stripp (edd.): *Codebreakers. The inside story of Bletchley Park*. Oxford.
12. Reynolds, David, (2005), *In Command of History. Churchill fighting and writing the Second World War*, New York.
13. Stafford, David, (1997), *Churchill and Secret Service*. London.
14. Taylor, A.J.P. (1965), *The Origins of the Second World War*, London, 1965.
15. Thucydides, (1956), *The Peloponnesian War*, I, 22, apud A.W. Gomme: An Historical Commentary on Thucydides, vol. I, p. 149, Oxford (first published 1944).
16. Wolters, Jo, (2003), Dossier Nordpol. Het Englandspiel onder de loep.
17. Woodhouse, C.M. (1982), *Something Ventured*, London.

RESILIENT CONCEPTS OF THE SOVIET ACTIVE MEASURES PROGRAM: DISINFORMATION, DECEPTION, FORGERIES. CASE STUDY: 1968 INVASION OF CZECHOSLOVAKIA

Mircea STAN[*]

Abstract

At the present time, the active measures program is perceived as a new structural innovation, conceived by the security and intelligence services of the eastern side of Europe, without taking into account its historical and evolutionary side.

The hypothesis of the article is that disinformation, deception and forgery, resilient concepts of the Soviet program of active measures, were real, sophisticated instruments that generated strategic events in order to create advantages for the Soviets in the short, medium and long term in the European field of security and defence. I have been following the logical and heuristic aspects of the research hypothesis: logical because they are a coherent conception of the past which also has implications today; heuristic, because the research enrols new data and information in the scientific circuit, from recently declassified archival documents, in order to discover and prove the truth.

In the elaboration of the article, I considered the research of the relational process between disinformation, deception, forgery and the historical phenomena they generated.

Keywords: *security, active measures, intelligence, disinformation, deception, forgeries.*

Introduction

Active measures, designed by the Soviets, have been and are real sophisticated instruments that generate strategic events in order to create short, medium and long term benefits at the social, political, military, economic, informational level, etc. There is no universally accepted definition for the concept of active measures, but they include

[*] PhD "Mihai Viteazul" National Intelligence Academy, email stanmircea90@gmail.com

disinformation, subversion, influence, propaganda, undercover operations, deception, rumours, manipulation, provocation, forgeries, diversion, **maskirovka** (Pirnie, 1985, 1-22; Keating, 1981, 1-20; Mitrokhin, 2004, 64-58)[1], reflexive control, sabotage, penetration, discretization, and the means by which they are achieved. To describe the complexity of the means of achieving the active measures we used, as an integrating term, the Soviet active measures program.

The Soviet active measures program is a counterpart to the irregular or unconventional warfare. In order to bring the definition of the active measures program to the present, we argue that it describes military and non-military irregular/unconventional methods of hybrid warfare. To better understand the current implications of the active measures program, it is necessary to present a retrospective of hybrid warfare.

Defining concepts: disinformation, deception, forgery – resilient concepts of the Soviet active measures program

Resilience is a concept that does not have the same meaning everywhere, but is increasingly used. It is currently used in a wider range of areas, institutions and organizations. Nor is the vast field of security an exception, resilience being a term used in more and more security strategies. Resilience studies offer a wider spectrum of reflection. For example, Liisa Välikangas proposes a new vision of resilience, arguing that the trends were to see resilience as a "backup solution", as the ability to return to the status quo before a disturbing shock/phenomenon occurred.

[1] A traditional Soviet term used in military operations. Maskirovka is a term used to describe a "mix" of deception, hiding, simulation, disinformation, false demonstration, camouflage, all meant to hide the real position of the troops and mislead the enemy, leading to inaccurate plans, forecasts and conclusions. In the KGB jargon, maskirovka describes a larger set of intelligence/counterintelligence actions such as: camouflage in surveillance (maskirovka v naruzhnom nablyudenii), camouflage of clandestine radio communication (maskirovka konspirativnoy radiosvyazi), and camouflage of microdot (maskirovka mikrotochki) – it refers to a small text or image printed on a disc to prevent its detection.

Another definition of resilience is the ability of a system/ systems to cope with unpredictable changes (Chakravarthy, 1982, 35-44). Recent sources define resilience as "the ability to avoid, minimize, resist, and recover from unforeseen, natural or man-made situations produced under all circumstances existing at that time".

In our case, a possible definition of resilience with reference to the three elements of the Soviet active measures program may be the following: the capacity of a system (the Soviet active measures program – the initiating State) to ensure and maintain the core mission at an acceptable and functional level (the purpose for which it was created) following the occurrence/intervention of unforeseen circumstances/ disturbing factors (from the state that is targeted/attacked) and the return, reconstruction or renewal of the situation thereafter.

Disinformation

Disinformation was one of the most used means in achieving the Soviet active measures. Conceptual delimitation of elements that make up the apparatus of active measures becomes a difficult task to achieve in the context of using these terms incorrectly and without discernment.

Trying to develop a definition of disinformation is a complicated process. The difficulty arises, first of all, from the fact that "it has extremely fluid borders with intoxication, influence, propaganda, subversion, manipulation" (Hentea, 2004, 46).

Disinformation has been manifested ever since the earliest times, however the term itself can be placed in the Soviet space at the beginning of the 20th century (West, 2006, 89; Lerner and Lerner eds., 2004, 331-335). In 1923, Arthur Artuzov (Haslan, 2016, *passim*) set up an office for disinformation within the GPU (**Gosudarstvennoye politicheskoye upravlenie** – the Soviet State Political Directorate from 1922 until 1923), "deza" being subsequently taken over by Iosif Unsliht, whose activity was centralized on January 11, 1923 (Haslan, 2016, 35-38). In the specific Soviet terminology disinformation (**dezinformatsionnyye svedeniya «dezinformatsiya»**) refers to "selected information which is transmitted to an opponent to create a false image about certain events which he could use to make

fundamental decisions". Also in Soviet terminology we find the term operative disinformation (**disinformatsiya operativnaya**) which refers to operational procedure consisting of providing the enemy with specific specially prepared information which will give a false picture of activity being undertaken by the counter-intelligence service (plans, forces, resources etc.) and may encourage the enemy to take decision which are advantageous to the counter-intelligence service (Mitrokhin, 2004, 193).

Disinformation started being used as early as 1959 as a term to define Soviet active measures (Parish, 2002, 93), which is not true since active measures refer to a wider range of elements, which has already been demonstrated.

Even though the KGB (**Komitet Gosudarstvennoi Bezopasnosti** – USSR's Committee for State Security, 1954-1991) was coryphaeus in the field, the Soviets did not hold exclusivity of disinformation, Nazi Germany and Fascist Italy being two of the disinformation craftsmen. During the Cold War, both camps (socialist and capitalist) practiced disinformation. For the French, disinformation was a "Intermittent or continuous action – using any means – that consists in misleading an adversary or favouring subversion in order to weaken it" (Cathala, 1991, 24), and for Anglo-Saxons disinformation meant "the process of presenting factual information in so as to induce the recipients to make the wrong conclusions" (Cole, 1998, 172).

The French took over the term "dezinformatsiya" in the 1970s, Vladimir Volkoff being the artisan of the field through his writings (Volkoff, 2007, 17). The "transfer" of disinformation from the security and intelligence services area to the mass-media area complicates things even further. Up to now, it has not been agreed that the concept should be given a definition of "wide use". In this sense, I argue that defining concepts is necessary, implicitly defining disinformation, but not in the sense of "forcing" a definition, but identifying in the previous definitions, starting from the general and going to specific, of the common elements and specific definitions.

Two of the disinformation theorists define it as "a manipulation of public opinion for political purposes, using information treated with distorted means" (Volkoff, 1999, 25) or a multitude of means aimed at

destabilizing a state or a society without necessarily calling for armed forces (Cathala, 1991, 24). Vladimir Volkoff proposes an approach to disinformation involving three elements:

"- a manipulation of public opinion, meaning intoxication;

- distorted means, meaning propaganda;

- domestic or foreign political purposes, meaning advertising" (Volkoff, 1999, 25).

For other authors, disinformation is "any intervention on the basic elements of a communication process, intervention that deliberately changes messages to determine in the receivers certain attitudes, reactions, actions desired by a particular social agent" (Zamfir, 1998, 167). From a French perspective, disinformation seeks to "create a false reality so convincing that the opponent thinks it right" (Nord, 1971, 17).

Starting from the model proposed by the Soviets and from the implementation of the actionable measures, disinformation was raised to the rank of doctrine in the USSR (**Soiuz Sovietskih Soţialisticeskih Respublik** – The Union of Soviet Socialist Republics, 1922-1991), whereby the entity who disinforms (the source/transmitter) transmits certain information (partially true) to the disinformed (receiver) (Volkoff, 2007, 16).

Disinformation is a long process that builds over time and shapes the consciousness of a segment of the population of a country or nation. Disinformation, as a long-term process, does not imply the action of persuading someone to believe what actually does not exist, but to provide hard or partially verifiable information supplemented by lies (Volkoff, 2007, 9-10).

Disinformation is a long-term doctrine/technique/process (Volkoff, 2007, 16; Hentea, 2005, 70-72) through which the disinformed is not deprived of information but rather false information is provided to it. The stages of disinformation are carefully planned, with every detail being carefully scrutinized. In order for a disinformation action to succeed, it must have thousands of hours worked back and rely less on the credulity or slowness of the masses or target group. Excessive disinformation actions are excluded to preserve the credibility of the author. The disinformation actions of the Soviet Union directed against

both opponents and partners turned against the Kremlin in many moments, especially when the Western states withdrew from international organizations created and sustained by Moscow. Disinformation should be used cautiously, otherwise it may have unfavourable consequences for its initiator.

Disinformation has some defining features: creating a false reality or as far from the truth as possible, carefully planned and elaborate as for the disinformed (state, organization or person) to consider it viable; it must always be done with the precise purpose of protecting sensitive information; seeks to destabilize the opponent's logic by directly disinforming the sources so that the disinformed can no longer verify the accuracy of the information.

Deception

Deception is another element of active measures with more implications in the military area. Most of the deception studies are of American origin and refer to strategic military deception (Department of the Navy, 1980, *passim;* Idem, 1986, 28-46; US Air Force, 1987, *passim*), but the first reference to deception is made by Sun Tzu who said "all warfare is based on deception" (Tzu, 1963, 66).

Deception has been the subject of many analyses of the US Army since the late '80s, belonging mainly to the US Navy Department. In a material developed in 1981, deception was defined as "deliberate misrepresentation of reality done to gain a competitive advantage" (Daniel et. al., 1980, 5). The same material distinguishes two variants of deception that produce different effects and work in different ways.

"The less elegant variety, termed «ambiguity-increasing» or «A-type», confuses a target in order that he be unsure as to what to believe. It seeks to compound the uncertainties confronting any state's attempt to determine its adversary's wartime intentions. Contradictory indicators, missing data, fast-moving events, time-lags between data-collection and analysis, change all in habit accurate intelligence assessments. (...) In contrast to deceptions increasing ambiguity, there is a second more complicated category which we label the «misleading» or «M-type». They reduce ambiguity by building up the attractiveness of the wrong alternative" (Daniel et. al., 1980, 8-10).

John Dziak captures very well the role and place of deception over Russian history: "Strategic deception, whether military or political, has been an integral feature of the Slavic tradition. Mongol methods of warfare masterfully deflected enemy attention toward false threats, a lesson absorbed by their Muscovite vassals and, in turn, their tsarist successors. The mirage quality of Russian political deception is captured by Potemkin's notorious «villages»" (Dziak, 1987, 3).

Other materials distinguish two large areas where the Soviets acted using deception as part of the active measures program. In the political field, where "political deception consists of efforts to influence the opinions of policy makers, opinion leaders and the general public in the West and the Third World" and the field of intelligence, where Intelligence deception is designed to affect an opponent's military planning and warfighting capability. This type of deception is maintained through misdirection of the perceptions, products, and recommendations of intelligence analysts regarding Soviet intentions and capabilities in military and political affairs (Walters, 1988, 12).

In the USAF (United States Air Force) materials, the authors believe that the Soviets have a complete definition for the art of deception: "Strategic cover and deception is accomplished upon the decision of the Supreme High Command and includes a set of measures for security in preparing strategic operations and campaigns, and also for disorienting the enemy with respect to the true intentions and actions of the armed forces (...). Methods for accomplishing cover and deception include: concealment, feints, simulation, and fabrication of information using communications media, the press, radio, broadcasting, television, etc. (...). It is emphasized that cover and deception measures should be continuous and realistic" (US Air Forece, 1986, 52-58).

One of the first seriously developed materials to deal with the subject of deception as an active measure is found in Cynthia M. Grabo's "Soviet Deception in the Czechoslovak Crisis" study. The author makes a radiograph of the deception that the Soviets planned to invade Czechoslovakia in 1968. It is interesting Cynthia M. Grabo's perspective on the thin line of demarcation between reality and deception that the

analyst will have to take into account in its materials. The work focuses on political, military, politico – military deception (Grabo, 1993).

Robert W. Pringle, author of the Soviet/Russian security and intelligence dictionary, defines deception as the term that denotes **maskirovka** (Pringle, 2006, 153), which I disagree with because **maskirovka** has a wider scope than deception, including other elements such as: camouflage, hiding, simulation, false demonstrations, and disinformation.

Barton Whaley, a prominent researcher and teacher in the field of studies and theories of the practice of deception and counter-deception defines deception as "any attempt – through words or actions – intended to distort the perception of reality of a person or group. And to keep things simple, a lie is any statement made with intention of deceiving" (Whaley, 2006, VII). Barton defines deception based on a typology of perception as follows: at the top of the pyramid is the perception that is divided into the wrong perception and correct perception. The wrong perception is subdivided into two subcategories: 1) induced by someone else, including deception (deliberate) and distortion (unintentional); 2) self-induced, comprising of self-deception and illusion (Whaley, 2006).

Forgeries

Forgeries were used by the Soviets to compromise people, local or central authorities, and even the domestic or foreign policy of the various target states. Forgeries (**falshivka)** refer to documents and are defined by the Soviets as follows: a report or false documents specifically designed on the basis of information that is known to be false, which is disseminated by mass propaganda to compromise the foreign or domestic policy of another state, the activity of its institutions or individuals (Mitrokhin, 2004, 139).

Mechanisms of implementing the soviet active measures program

The mechanism of cooperation for implementing the program of active measures followed this path: Department "D"/Service "A" (Watts,

2011, 302; Schoen and Lamb, 2012, 19)[2] worked with the Foreign Affairs Section of the Central Committee of the Communist Party of the Soviet Union (CC of the CPSU)/Foreign Affairs Sections of the Central Committees of the other communist parties in socialist countries, the Propaganda Section of the CC of the CPSU/Propaganda Sections of the other communist parties in socialist countries, the Soviet Academy of Science/Science Academies of the other socialist countries, the PGU (**Pervoe Glavnoe Upravlenie** – the First Main/Central Directorate – Foreign Intelligence, soviet espionage, 1954-1991) residences and the written and audio-visual press.

Within PGU residences, the mechanism of cooperation was provided by the "PR Line", which was in charge of economic and political information, military strategy and active measures (Mitrokhin and Andrew, 2003, 570; Idem, 2006, 454). According to a former officer of Service "A", who defected to the USA in 1979, the active measures program was not implemented outside the Soviet borders by Service "A" officers. Instead, this mission was given to the "PR Line" staff along with precise instructions. Also, Service "A" used to draft a bulletin which contained secret information. The bulletin was given to the members of the CPSU Politburo. It included specific details of certain active measures programs or other operations that were already successfully implemented (Barron, 1983, 449).

Department "D" also used to cooperate with the residencies of security and intelligence services of other socialist countries, the Foreign Affairs Sections and the Academies of Science of those respective states. However, no actions were ever performed outside of KGB orders (Knight, 1990, 286).

---

[2] After the Second World War, the active measures program became more significant for the Soviets as special emphasis was placed on disinformation. For this reason, in 1959, Department "D" (Dezinformatsia) was established within the PGU and tasked with taking over and implementing all the active measures operations. There is conflicting data regarding the establishment of Department "D". Some sources support a version in which Service "A" (Slujba Aktivnik Meropriatil or the Service of Active Measures) became the successor of Department "D" (Dezinformatsia) in 1962. Other sources indicate that Service "A" became the successor of the Department "D" in 1971, at a time when the department included 700 officers and a KGB general was in charge of it.

Throghout the Cold War, the USSR had the advantage of receiving the support of powerful socialist parties in Western countries, especially France and Italy. The implementation of active measures was supported by Soviet advisers (Bittman, 1972, 45) placed in intelligence and military structures and the Cominform (1946-1956) (Duroselle, 2006, 352)[3]. After the dissolution of the latter, the same role was given to the Foreign Affairs Sections of communist and working-class parties in socialist countries. Between 1959 and 1965, the KGB "exported" its program of active measures to the other security and intelligence services of the WTO member states (Bittman, 1972, 142) except Romania.

The case of the Czechoslovak Socialist Republic (CSR)

Near the CSR occupation, the KGB suffers some transformations that cannot be neglected. Brezhnev's arrival at the head of the CPSU and the appointment of Andropov under the command of the KGB in May 1967 meant a change of USSR's actions in foreign policy. Brezhnev will not agree with Khrushchev's policy of "allowing" the socialist countries to move away from socialist dogma. It is an "ideological subversion" that Brezhnev and Adropov accused of being allowed by the old leadership. The Politburo, at Andropov's initiative, approved the establishment in the KGB of a directorate with five sub-directorates to fight against ideological subversion. In addition to the opening of new KGB offices internally, Politburo's P47/97-op decision entailed an increase in the total number of KGB staff to 2,250 employees, of which 1,750 officers and 100 officers appointed to the KGB at Lubianka. Changes have also been made to the KGB's XIth Department dealing with relations with the socialist countries. It had been an independent unit to the PGU and was reintegrated to Soviet espionage following another Politburo resolution adopted on 4 June 1968. Andropov mentioned that this was necessary as a result of the inefficiency of the XIth Directorate,

[3] It was founded on September 22th 1947. Its headquarters was in Belgrad. The Cominform had to ensure that links were created between European communist and working-class parties. It was designed like an "Information Office of Communist and Workers' Parties". The Cominform had lots of information on how the "popular democracies" were established.

whose activity degenerated to "simple protocol collaboration" without exchanging and processing important information and dealing only with the hosting of the homologous delegations from other socialist countries (Petrov, 2009, 146-147).

After 51 years since the Warsaw Treaty Organization (WTO) member troops invasion of the CSR and the declassification of numerous archive funds, the event itself reveals that the USSR has taken active measures through disinformation, deception and forgery at least from middle July (the beginning of the troop mobilizations that preceded the actual invasion) in order to convey to the entire world and particularly to the CSR that there will be no invasion. In the preparation of the invasion a variety of means were used to implement active measures from the political-diplomatic channels to the KGB-GRU (**Glavnoe Razvedîvatelnoe Upravlenie** – the Soviet military espionage service or the Main Intelligence Directorate) security and information services. The most commonly used explanations of the Soviets for the upcoming invasion referred to the fact that the massing of troops at the CSR border was done only for manoeuvre. Masking preparations under the disguise of manoeuvres was a *sine qua non* condition of the invasion.

From my point of view, Cynthia Grabo best captures the importance, scale and mechanisms that preceded the invasion as part of active measures: "True military deception, as opposed to the various means described above, is the most difficult and complex of all types of deception to orchestrate, at least on a large scale. It is most commonly used when hostilities are already in progress, when it may be used with other deception measures to disguise the scale of a build-up, the date or place of attack, and/or to lead the enemy to believe that an attack is planned in one area when in fact it is not (...). The planting of false reports, through established intelligence channels or the diplomatic service, may be used as a part of the political or military deception methods described above. A military attaché is a useful channel for putting out a seemingly plausible explanation or disclaimer concerning a troop build-up, as is a diplomat to provide a false political story. These channels, along with the professional clandestine services, also may be used simply to flood the market with a mass of conflicting stories and

reports. Particularly when reports are sensational but otherwise appear to have some authenticity, they can be a tremendous distraction. If the volume of such planted disinformation is large enough, the analytical system can be so overwhelmed by it that the truly reliable or useful intelligence may become lost in the mill" (Grabo, 1993).

The entry of WTO member countries' troops into CSR has also been facilitated from a different angle. The Czechoslovak army continued to send army officers to specialize in the USSR where they were subjected to the KGB-GRU recruitment, and the Czechoslovak military intelligence service was directly "subordinate" to the GRU (Suvorov, 1984, 34) and took part in the security and defence decisions taken inside WTO. The full integration of the Czechoslovak Army within WTO has led to a detailed knowledge of the Kremlin needed in order to prepare the invasion. Near the intervention, the Romanian security and intelligence services reported the existence of: «numerous troops and weapons concentrations along the northern border» and diplomats from the embassies of WTO member countries accredited in Bucharest «acted as covered agents, collecting information on Romania's internal situation» (Retegan, 2000, 192-193).

The various political leaders from the Kremlin have always been sensitive to the minor deviations from the ideological concepts that the USSR has implemented in Eastern Europe, and Czechoslovakia, a country with a democratic tradition, has been imposed a regime in flagrant contradiction with its history. The path of reforms that the CSR will follow in 1968, where the dominant element was the rehabilitation of victims during Stalin's leadership (started during Khrushchev's time), was rejected by Brezhnev (Petrov, 2009, 145).

The year 1968 has major implications for the security environment of Central and Eastern Europe. Within the Soviet sphere of influence there was a split that divided the European socialist world into two camps: in the first one there were Yugoslavia, Romania, Albania and Czechoslovakia, and in the second, the USSR, Poland, the Democratic Republic of Germany, Hungary, Bulgaria. In the case of the first camp, I highlight a few aspects: firstly, the common visions of Belgrade, Bucharest and Prague over some problems were not due to the same internal criteria and they had not evolved the same over time.

Yugoslavia, although it had adopted communism openly, remained an "unaligned" state with an open economy, and in which the West saw a possible ally. Romania had started on the path of reforms and promoted a foreign policy different from that of Moscow, and Czechoslovakia joined the process of economic, political, social reconversion. Secondly, the question arises whether Tito, Ceausescu and Alexander Dubček really believed that their countries were separate entities within the socialist camp, or the revival of a "Little Entente" was just another projection of the Soviet active measures program meant to provoke a counter-reaction from the other Kremlin partner countries.

The security and intelligence services of the USSR acted during the 1968 CSR events through the active measures program. The most used elements were disinformation, deception and forgery in order to present a false reality to the international public opinion a false reality, contrary to the existing one.

Romania was the only member country of WTO that firmly opposed the invasion because the manoeuvre violated two of the elements that Bucharest has been promoting since 1964: national sovereignty and the right to decide in domestic politics. The fact that in 1968, and a few years after, Romania was part of the plans of a possible invasion, it was a risk that the country assumed.

Conclusions

Whether it is Medieval Russia, Imperial Russia, the Soviet Union, or the Russian Federation, history has shown that the relations of these expansionist state actors with the countries of Eastern Europe have been dominated, with some exceptions, by conflicts at the expense of cooperation. The expansionary tendencies of Medieval Russia / Imperial Russia / Soviet Union / Russian Federation can be explained by a strong sense of insecurity, visible today. Territorial expansion was the key to building a strong state and ensuring security for Russia, which has been reflected in its foreign policy since the interwar period. The logic of the "conquests" of the various states in Central and Eastern Europe is part of the "glacis / protection grid" tag, i.e. the building of security through territorial conquest, carried out in two stages: 1) 1939-1940 by signing the Ribbentrop-Molotov Pact; 2) 1944-1949

through the Red Army conquests and the conscious giveaways of the Anglo-Americans. The Russian conquests "tradition" is rather the result of a feeling of insecurity to the detriment of security, even in the current form of the Russian Federation.

The Soviet active measures program has reached its goal in the case of Czechoslovakia. Disinformation, deception, forgery made it possible for WTO member countries troops to enter, except for Romania, although political and diplomatic channels often expressed that the USSR did not intend to do so. In other words, the program of active measures, another "tradition" of the USSR succeeded, until the very moment of the invasion, to offer another "reality" to international public opinion, that of non-intervention.

References:

1. Barron, John, (1983), *KGB Today: The Hidden Hand,* New York, Reader's Digest Press.

2. Bittman, Ladislav, (1972), *The Deception Game: Czechoslovak Intelligence in the Soviet Political Warfare*, Siracusa, Syracuse University Research Corporation.

3. Cathala, Henri – Pierre, (1991), *Epoca dezinformării*, translated by Nicolae Bărbulescu, Bucureşti, Editura Militară.

4. Chakravarthy, Balaji S., (January 1982), „Adaptation: A Promising Methaphor for Strategic Management" in *The Academy of Management Review*, vol. 7, No. 1.

5. Cole, Robert (ed.), (1998), *International Encyclopaedia of Propaganda*, Chicago and London, Fitzroy Dearborn Publishers.

6. Daniel, Donald C., et. al., (May 1980), *Multidisciplinary Perspectives on Military Deception*, Department of the Navy – Naval Postgraduate School, Monterey, California.

7. Department of the Navy, (May 1980), *Multidisciplinary Perspectives in Military Deception*, Monterey, California.

8. Department of the Navy, (March 1988), Naval Postgraduate School, Monterey, California.

9. Department of the Navy, (December 1986), *Threat and Opportunity: The Soviet View of the Strategic Defense Initiative*, Monterey, California.

10. Duroselle, Jean – Baptiste, (2006), *Istoria relațiilor internaționale 1919-1947*, vol. I, translated from French by Anca Airinei, Bucharest, Ed. Științelor Sociale și Politice.

11. Dziak, John, (1987), „Soviet Deception: the Organizational and Operational Tradition", in *Soviet Strategic Deception*, Lexington Books, Lexington.

12. Grabo, Cynthia M., „Soviet Deception in the Czechoslovak Crisis", in *CIA*, Centre for the Study of Intelligence, vol. 14, no. 1, declassified on 22 September 1993.

13. Haslam, Jonathan, (2016), *O nouă istorie a serviciilor secrete sovietice*, translated by Ioana Aneci, Iași, Polirom.

14. Hentea, Călin, (2004), *Arme care nu ucid*, Bucharest, Nemira.

15. Hentea, Călin, (2015), *Propaganda și rudele sale: mic dicționar enciclopedic*, Bucharest Military Printing House.

16. Keating, Kenneth C., (1981), *Maskirovka: The Soviet System of Camouflage*, Germany, U.S. Army Russian Institute, Garmisch.

17. Knight, Amy W., (1990), *The KGB: Police and Politics in the Soviet Union*, Boston, Unwin Hyman.

18. Lerner, K. Lee, Lerner, Brenda Wilmoth (eds.), (2004), *Encyclopedia of Espionage, Intelligence and Security*, vol. 1, A-E, SUA, Gale.

19. Mitrokhin, Vasily, (2004), *KGB Lexicon: the Soviet intelligence officer's handbook*, London, Routledge.

20. Mitrokihn, Vasili, Andrew, Christopher, (2003), *Arhiva Mitrokhin: KGB în Europa și în Vest*, translated by Ion Aramă, Bucharest, Orizonturi Printing House.

21. Mitrokihn, Vasili, Andrew, Christopher, (2006), *Arhiva Mitrokhin: KGB-ul în lume*, vol. II, translated by Anca Irimia Ionescu, Bucharest, Orizonturi Printing House.

22. Nord, Pierre, (1971), *L'intoxication, arme absolue de la guerre subversive*, Livre de poche, Paris, Fayard.

23. Parish, Thomas, (2002), *Enciclopedia Războiului Rece*, translated by Ion Nastasia, Bucharest, Univers Enciclopedic.

24. Petrov, Nikita, (2009), „The KGB and the Czechoslovak Crisis of 1968: Preconditions for the Soviet Invasion and Occupation of Czechoslovakia", in Günter Bischof, Stefan Karner and Peter Ruggenthaler (eds.), *The Prague Spring and the Warsaw Pact Invasion of Czechoslovakia in 1968*, USA, Lexington Books.

25. Pirnie, Bruce R., (1985), *Soviet Deception Operations in World War II*, Washington D.C., U.S. Army Centre of Military History.

26. Pringle, Robert W., (2006), *Historical dictionary of Russian and Soviet Intelligence*, USA, Scarecrow Press.

27. Retegan, Mihai, (2000), *În umbra Primăverii de la Praga: Politica externă a României și criza din Cehoslovacia din 1968*, *Iași*, Romanian Studies Centre.

28. Schoen, Fletcher and J. Lamb, Christopher, (June 2012), *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*, Institute for National Strategic Studies, Washington D.C.

29. Suvorov, Victor, (1984), *Inside the Soviet Military Intelligence*, New York, Macmillan.

30. US Air Force, (May 1987), *An Historical Investigation of Soviet Strategic Deception*.

31. US Air Force, (1986), *National Security Policy Casebook*, USAF Air University.

32. Walters, Cathy Darlene, *Perceptions Management: Soviet Deceptions and its Implications for National Security.*

33. Volkoff, Vladimir, (1999), *Tratat de dezinformare. De la Calul Troian la Internet*, translated by Mihnea Columbeanu, Bucharest, Antet Printing House.

34. Volkoff, Vladimir, (2007), *Dezinformarea văzută din Est*, translated by Nicolae Baltă, Bucharest, Pro Printing House.

35. Watts, Larry L., (2011), *Ferește-mă, Doamne, de prieteni ....Războiul clandestin al Blocului Sovietic cu România*, translated by Camelia Diaconescu, Bucharest, RAO.

36. West, Nigel, (2006), *Historical Dictionary of International Intelligence*, Lanham, Maryland, Toronto, Oxford, The Scarecrow Press Inc.

37. Whaley, Barton, (March 2006), *Detecting Deception: A Bibliography of Counterdeception Across Time, Cultures, and Disciplines*, second edition, Foreign Denial and Deception Committee, Washington DC.

38. Wu Tzu, Sun, (1963), *The Art of War*, translated by Samuel B. Griffith, the Oxford University Press, London.

39. Zamfir, Cătălin (coord.), (1998), *Dicționar de sociologie*, Bucharest, Babel Printing House.

INTELLIGENCE AND SECURITY IN THE 21ST CENTURY

MEDIA LITERACY AS A RESPONSE TO FAKE NEWS

Dana SÎRBU*

Abstract

Critical thinking and media literacy programs are essential to increase citizens' resilience to fake news. The purpose of this paper is to illustrate the role of media literacy in combating disinformation and propaganda. Also, the article highlights the importance of media literacy in the contemporary world; the characteristics of media literacy and several recommendations and strategies that aim to develop critical thinking of the individuals, especially for the young generation. Although critical thinking and media literacy are long-term solutions, their application will eventually improve and strengthen a democratic society. It is important to learn how to identify and recognize fake news, to know the reasons and mechanisms behind the spread of fake content in the online environment and to understand the necessity of verifying the accuracy of the information before sharing it with others.

Keywords: *critical thinking, media literacy, fake news.*

Introduction

In the last few years, the fake news phenomenon has seen tremendous public attention especially in the context of the US elections in 2016. Also, in 2017, Collins, an online English Dictionary has proclaimed the term "fake news" the word of the year. In the same way, at a simple search on Google, we will see that the results associated with fake news concept are about 907.000.000. Despite this notoriety, societies are not yet ready to face the new challenges associated with this issue. This happens in the context brought by the development of new technologies and the complexity of algorithms that make it impossible for human beings to detect false messages and disinformation in the online environment.

* PhD Student, "Mihai Viteazul" National Intelligence Academy.

A brief historical overview will reveal that starting with the Ancient world and going through the modern times, fake news or disinformation has been a constant throughout all the important and revolutionary moments of the international community. Despite the fact that the phenomenon we are talking about is not new at all, societies have to find tailored solutions adapted to the rapid evolutions of the world. More and more specialists are developing new partnerships in order to create a protective environment for the incoming generation and for the students who are in the early years of school. For example, National Education Association [1] from USA has developed the concept of the four 'C' – Communication, Collaboration, Critical Thinking and Creativity – skills which could be seen as the premises for 21st century education. Also, if we are to consider the increased number of messages that circulates online on social media platforms and the behaviour of people in some cases – like redistributing news without checking it or even reading it – the long term effects will conduct to a chaos of information. In a study[2] from 2017 the authors are talking about concepts like "eco chambers", "filter bubble", "confirmation bias", or, broadly speaking, "information disorder". In the large spectrum of information disorder, some authors include three types: Dis-information, Mis-information and Mal-information.

In this context, the most frequent question is: What can we do? How can we teach young generations of people to deal with disinformation, propaganda and fake news? Media literacy has become more and more used as a universal response to this very complex phenomenon. As we mentioned before, this type of threat to liberal democracies is not new at all, but will become more sophisticated as the development of artificial intelligence will bring more technological possibilities to multiply and share messages on a larger scale or to create automatic computers to generate and create news. The European Union has adopted an Action Plan against Disinformation in order to

[1] See more on www.nea.org.

[2] For more information, see C. Claire Wardle and Hossein Derakhshan: Information disorder: toward an interdisciplinary framework for research and policy making, Council of Europe report DGI (2017)09, available at https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c.

fight against disinformation, fake news and propaganda in order to consolidate resilience of the European societies against this kind of hybrid threat. Regarding this, some researchers concluded that "falsehood diffused significantly farther, faster, deeper, and more broadly than the truth in all categories. The effects were most pronounced for false political news than for news about terrorism, natural disasters, science, urban legends, or financial information" (Vosoughi, Roy and Aral 2018). Also, the role of media literacy becomes more important especially in a context in which the development of the fake news phenomenon generates a crisis for contemporary society and threatens the good functioning of liberal democracies.

The importance of media literacy in the 21st century

The technological revolution and the spread of the Internet have reconfigured how we have access to information and redefine the role of the press. In a world where information it is very accessible, the role of selecting it becomes an essential quality for each of us. As we all know, fake news, disinformation or propaganda represent a threat to liberal democracies, and some of the effects regarding this phenomenon include diminishing confidence in state institutions and confusion during electoral cycles. "A community is a healthy democratic community – it is an ≪informed community≫ – when digital and media literacy are widely taught in schools, public libraries and other community centres" (The Knight Commission 2009). Thus, as a whole, society must provide the premises for an optimal development for young people, especially in terms of education. This becomes even more important as technology influences the teaching and learning process. Students have a lot of information that can be difficult to manage and which they cannot analyse it properly. For this, the role of media literacy becomes crucial in an era of informational abundance. "The traditional way of learning has therefore changed. Learning is no longer seen as an activity restricted to school settings since it went online, and that is why it is now understood (or should be understood) as a process that is disorderly, hazy, informal, chaotic, continuous, digital, lifelong and based on the power of online connections" (Blanco, Nuere, & Martín, 2013, pp. 55-56) .

When we refer to media literacy, we are talking about "the ability to access, analyse, evaluate, create, and act using all forms of communication are interdisciplinary by nature" (National Association for Media Literacy and Education, n.d.). The Media Literacy Expert Group of EU defines media literacy as an inclusion of "all technical, cognitive, social, civic and creative capacities that allow a citizen to access, have a critical understanding of the media and interact with it"[3]. Also, media literacy involves learning to "read" the media through critical analysis, evaluation and reflection. Media literacy involves a broader understanding of the social, economic and institutional communication context and the way in which they influence the experiences and actions of people. The citizen who consumes the media adequately, rationally and in an assumed manner should be the new societal model in a world of emerging needs. If young people have analytical skills and they are critically accountable to all media messages, through a real capacity to make decisions, they cannot be manipulated by propaganda or disinformation. All the adult trainers (parents, tutors, teachers, experts, methodologists, etc.) have an important role in developing and expanding the concept of media literacy in order to ensure the premises of an adequate education for young generations. In this sense, it is important for the society to adopt a new formula in order to create literate citizens. For instance, there are some authors who claims that "we must consider new approaches to teaching and learning about media that focus intentionally on the civic: how we can use media to reform communities, to create meaningful human interactions, and to build sustainable pathways for positive social impact" (P.Mihailidis 2018). Also, the importance of media literacy it`s highlighted by Gallagher who considers that "media literacy is important because it is the basis for being an informed and critical

[3] For more information, see https://ec.europa.eu/digital-single-market/en/news/meetings-media-literacy-expert-group.

thinker in a world where technology and media are ubiquitous, helping to immunize people against undue persuasion and false information" (Gallagher, J.D., Magid, & Ed.D, 2017).

The Media Literacy Group Expert of UE was set up to meet the most pressing issues related to the development and implementation of media literacy process. In this regard, the working group experts "identify, document and extend good practices in the field of media literacy; facilitate networking between different stakeholders, with the aim of cross-fertilization; explore synergies between different EU policies and support programs and media literacy initiatives" (Digital Single Market, n.d.).

More than that, it is necessary to introduce media training programs in schools, especially in secondary education, to promote a lucid and critical attitude among media users regarding media coverage and to promote quality journalism. Also, media literacy is necessary in order to combat misperceptions, prejudices and hate-speech. Before an actual implementation of a media literacy program, one should first establish a conceptual and legislative framework on the basis of which the media literacy program should function. Thus, taking into account the cultural, national and local specificity, the government should establish the best approach to implementing the program together with the civil society and educational institutions. For example, if a community is more likely to watch TV than to read, then media education should use all media channels to convey the message to that community.

At the same time, media literacy is important for democracy and for ensuring a secure information environment. As it has been observed lately, misinformation and distortion of truth around some important events, such as electoral cycles, create confusion among voters and pose a threat to liberal democracy. That is why media literacy plays a role in protecting democracy and democratic processes. Media literacy can also play a role in preventing individuals from adhering to extremist and violent ideologies, and may be a barrier against extremist messages.

The desideratum of media literacy is to create citizens who are responsible for their choices and their opinions. At the same time, media literacy is important to maintain ethical values when creating and disseminating media content across all social media channels. Hence, a literate citizen will have these values and principles, such as sincerity and impartiality.

Strategies and techniques related to media literacy and critical thinking

Young people are more prone to using social media messages, and the educational process should be geared toward inoculating skills for detecting false news and propaganda messages. Preparing them to develop skills related to searching on the Internet and abilities for checking the accuracy of information should begin as early as possible and continue throughout the educational and professional life. The starting point should be developing media and digital competences among young people, introducing media literacy in schools, institutions and organizations, developing cooperation between the private and public sectors.

Also, there are some authors who brings into discussion the role of the teachers in the process of building critical thinking among students: "educators have a responsibility towards their students to foster critical thinking for evaluating information, which in turn informs their decision making. The ability to distinguish truth from falsehood is important in many contexts and at many levels i.e. the personal, group, project, organizational, political, and societal" (Georgiadou, et al. 2018, 3). In the same manner, Hobs argues that "people need the ability to access, analyse and engage in critical thinking about the array of messages they receive and send in order to make informed decisions about the everyday issues they face regarding health, work, politics and leisure" (Hobs 2010, 7).

First of all, media literacy, inevitable, involves critical thinking. Broadly speaking, critical thinking means to constantly analyse and

evaluate the information, making judgments based on facts and proofs. "Critical thinking is self-directed, self-disciplined, self-monitored, and self-corrective thinking" (The Foundation for Critical Thinking, n.d.). "Critical thinking consists of an awareness of a set of interrelated critical questions, plus the ability and willingness to ask and answer them at appropriate times" (Browne & Keely, 2007, p. 3).

Developing critical thinking does not only benefit the trained individuals but also the society they are part of. Critical thinking heals a society of prejudice and passivity, making political and social concepts more accessible and making participants more aware and involved.

Teacher training courses are also required so that they have the necessary knowledge to convey to their students. At the same time, teachers and trainers have a role to play in supporting governmental structures in developing specific policy proposals and educational initiatives, especially in media literacy. This leads to increasing citizens' resilience to misinformation and false news as well as to strengthening critical thinking and improving learning through the integration of new technologies into teaching.

As we pointed out throughout this paper, teachers have an important role in developing student critical thinking. Here are some methods and strategies such as:

Analysing the content of media messages – The teachers could start developing lessons in order to improve a student`s capacity and skills for questioning media content. Priority should be given to the development of techniques, both technological and theoretical.

Socratic Method – Socrates, a philosopher and professor in ancient Greece, believed that disciplined practice of questions gives the student the opportunity to reason logically and to determine the validity of some ideas. "The oldest, and still the most powerful, teaching tactic for fostering critical thinking is Socratic teaching. In Socratic teaching we focus on giving students questions, not answers." (Paul & Elder, 1997).

Through this technique, the professor claims that the subject is not known for him and begins a discussion with students. In this way, the teacher will analyse the arguments and the knowledge possessed by students. The Socratic Method starts from the idea that each person has

the logical ability to understand and find out any answer. The main advantage of this method is that each student is actively involved in the learning process, which is a personal effort.

Individual Learning Plans – Learning plans must be adapted to the age and understanding of the individual, so that the information transmitted can be properly received and understood. Facing History and Ourselves, a non-profit international educational and professional development organization, provides information and individual learning plans on the role of media literacy to the general public. Through key questions, citizens can develop certain skills to evaluate the information they encounter: "How does social media shape our relationship to and understanding of breaking news events?" "What is the relationship between social media and the practice of quality journalism?" "How do we know if information shared on social media is credible?" Using these questions as a starting point, students explore a variety of topics, including the impact of media on the population, in terms of confirmation bias and stereotypes, and the impact of social media on mainstream news media and public opinion.

"Many news organizations, including PBS News Hour and the New York Times, have also published lesson plans designed to help students develop the habits of mind necessary to critically evaluate online news content" (Holmes, 2018).

Game Media Literacy – This is a concept defined as "educational processes that are specific to games. These processes specifically include learning that takes place while playing games, education that takes place while designing games, learning about games and learning from games how to teach" (Swertz, 2016, p. 1). A game is the simplest way to learn and practice certain skills.

Reading laterally – Means consulting, reading and looking for third-party sources to verify the information in terms of precision, truth and credibility.

A study by experts at Stanford University, which tracked how different participants, including academics such as history teachers, fake news experts and students assess the credibility of online sources, found that:

"Historians and students often felt victim to easily manipulated features of websites, such as official-looking logos and domain names. They read vertically, staying within a website to evaluate its reliability. In contrast, fact checkers read laterally, leaving a site after a quick scan and opening up new browser tabs in order to judge the credibility of the original site. Compared to the other groups, fact checkers arrived at more warranted conclusions in a fraction of the time (Wineburg & McGre, 2018, p. 2)".

The authors explain that those who have been able to best evaluate sources – fact-checking experts – have used what is called *lateral reading*, and they have checked other sources available about the site in question instead of analysing the same site.

Before implementing media literacy strategies and methods, it is important to remember that the role for their effectiveness is shared between communities, school, local, regional, and international authorities. A media literacy strategy must continue throughout the educational process of students and pupils so that they become responsible adults when interacting with social media and online news/ messages. For this, it is necessary for them to have developed critical thinking and be aware of the simple error of judgment, to distinguish between facts and opinions, to have a logic based on interpretation and analysis, depending on context and event. At the same time, it is necessary for parents to continue the educational process at home and to provide time for activities related to online content and not only. The authorities, in their turn, have the task of allocating financial resources to implement such strategies: campaigns to raise awareness about fake news and to promote the role of media literacy, introducing school curricula dedicated to this theme or summer school for students.

On the other hand, there are some opinions stating that "is not sufficient to simply raise awareness about how and why certain news is produced and consumed, but it is also necessary that authorities take a more active role in regulating the distribution of that information rather than hoping that millions of people will fast become media-wise" (Celot, 2018).

Wardle and Derakhshan argue that the long-term implications of misinformation campaigns are specifically created to spread distrust

and confusion and to intensify already existing socio-cultural divisions, using nationalistic, ethnic, racial and religious tensions as instruments (Wardle & Derakhshan, 2017). Another critical aspect is that popular social networks make it difficult for people to evaluate the credibility of any message as the content looks almost identical. This means that people increasingly rely on friends and family members to guide them through the informational space.

As Messing and Westwood have argued, "social media has had two effects: by combining stories from multiple sources, the emphasis is on the story, not on the source, secondly, social recommendations and approvals guide readers," rather than checking and analysing (S.Messing & Westwood, 2014). Social media has had a profound impact on how people are discussing current issues and engaging with politics. The presence on these platforms helps young people to independently cultivate a political identity and provides people of all ages with personalized civic knowledge both in authoritarian and democratic regimes. Large-scale moves were born, organized and broadcasted on platforms such as Facebook, YouTube, WhatsApp, FireChat and Twitter. Positive and widespread democratic social media potential is widely discussed, but we must be aware that at the same time there could be another dark side of this new technology (Woolley & Howard, 2016).

Social media has become a powerful tool for propaganda because interactive social networking sites provide a powerful platform for debate and sharing of opinions. Propaganda, in the form of a YouTube uploaded video, a post on Facebook or Twitter, or even a comment, has a great deal of efficacy to disseminate certain values and beliefs.

Fake news phenomenon is a global issue, and global scale solutions are therefore needed. Several countries, including France, Germany, Singapore and Malaysia have implemented laws to counter fake information, but these efforts are likely to be unproductive if they are not integrated into a wider perspective. To build a successful strategy capable of rebuilding the truth, an exhaustive approach must be multifaceted and inclusive, and efforts should be synchronized in a perfect understanding of the issue and effective long-term results.

It is important to understand first of all how fake news works and how technology facilitates their spread. Moreover, a valid strategy should address the fake news phenomenon in a differentiated manner, since a singular approach to fake news runs the risk of creating limitations.

Scientific studies[4] demonstrate that exposure to disinformation or conspiracy theories leads to alteration of perception, also affecting the decision-making process. For example, in 2014, the University of Kent conducted such a study, demonstrating that parents exposed to a conspiracy theory about the negative effects of vaccination decided not to vaccinate their children, while parents who were provided complete information, including about the falsity of conspiracy theories, and have accepted vaccination.

Also, the process of thinking and evaluating the sources becomes essential in a world dominated by too much information. As Browne and Keely sustain, "thinking carefully is always an unfinished project, a story looking for an ending that will never arrive. Critical questions provide a stimulus and direction for critical thinking; they move us forward toward a continual, ongoing search for better opinions, decisions, or judgments" (Browne & Keely, 2007, p. 2).

On the other hand, Facione goes further and adds two more characteristics of a critical thinker: "Beyond being able to interpret, analyse, evaluate and infer, strong critical thinkers can do two more things. They can explain what they think and how they arrived at that judgment. And, they can apply their powers of critical thinking to themselves and improve on their previous opinions. These two skills are called "explanation" and "self-regulation" (Facione, 1992, p. 6).

Media literacy beyond elementary skills

The main dimensions of media literacy should go further than skills and competencies as abstract notions. Renee Hobs, an expert on

[4] For more information see Daniel Jolley et al., *The Effects of Anti-Vaccine Conspiracy Theories on Vaccination Intentions*, PloS, vol. 9, nr.2, 2014.

media literacy, proposes five essential elements of media literacy: access, analyse, create, reflect and act (Hobs, 2011, p. 123). According to her, it is important to know how to use media tools in an adequate manner, by appealing to critical thinking, creativity, collaboratively and, also, "applying social responsibility and ethical principles to our own identity, communication behaviour" (Hobs, 2011, p. 12).

The goal of media literacy is to bring a change in the online behaviour of individuals in terms of reading, analysing and sharing messages, especially in the online environment and on social media platforms. Unfortunately, the Internet has reconfigured how we relate to events and news, most of the time this information being already analysed by others. In this way we are much more influenced by the first article/information we read.

Moreover, psychologists warns us that people will look for that information that already confirms their own predispositions, so that the message they adhere to is the one that validates their own conception of the world and life in general. Cognitive bias is a thinking mechanism, which involves a systematic distortion of judgment/rationality in relation to reality, and which can make an individual have different attitudes to facts of the same nature, that is, to have a paradoxical behaviour, contradictory, inexplicably logical. By learning to recognize a cognitive bias, we can avoid a lot of mistakes, improve our memory, affective reactions, and be in control of our identity and value. Thus, the role of media literacy should be understood in terms of behavioural impact and attitudinal change. The more this education and training will be achieved, i.e. from the youngest age, the better prepared adults will be better prepared for the informational environment of the 21st century.

Although we cannot predict how the concept of information will be reconfigured over 50 or 100 years, it is important to know how to relate to what we read every day. Although so-called *deep fake* and *computational propaganda* are at the beginning of the road and become complex and difficult to detect, the internet user will be better prepared if he or she has a minimum of training and knows how to relate to that news or message.

For this, some features that media literacy has developed are essential, including scepticism and the ability to be aware of our own

cognitive biases. People should have that impetus that determines them to look for other sources to have another approach. At the same time, media literacy also means progress beyond the capacity to analyse social media and beyond value based judgments; media literacy should also mean innovation and involvement. The communities need innovation and solutions to address the information challenges of contemporary society. Individuals need to get more involved in implementing and promoting media literacy anywhere and anytime when they have the opportunity. The role for implementing solution to increase awareness among societies should be divided and shared among all actors and participants in public life. In this context, the citizens themselves can dictate the progress and the changes that are challenged to progress.

Media literacy should promote values such as good governance, social inclusion, diversity and media autonomy. Given the recent events and anti-European discourses, these values are very necessary and must be included in media literacy programs.

At the same time, media literacy should be centered on developing research, methodologies and working tools in action areas such as freedom of expression, anti-discrimination, communication campaigns, and public events that promotes the values of liberal democracy. The role of media literacy, beyond being able to identify disinformation, should go to the development of creativity in media communication.

As we have highlighted above, social media is becoming more and more a primary source of information, especially for young people. They, as well as other citizens, must be able to distinguish between credible and less credible sources of information. Therefore, initiatives aimed at increasing the level of media literacy are essential. Interactive training and workshops for media consumers should be supported and developed to improve information standards.

Finally, the improvement of education systems around the world is based on cooperation and information sharing about the best practices and lessons learned, to stimulate the development of

programs and initiatives to implement media literacy. The young generation can benefit from new educational tools and practices that will provide them with a new understanding and approach to the online environment.

Media literacy should not only be taught in schools, but by all possible audience channels. For example, media literacy on TV or radio programs could be introduced. YouTube special channels or blogs that promote this concept could also be created for young people. It is well known that young people tend to mimic behaviours. Therefore, if celebrities promote the concept of media literacy and popularize it among young people, they would be more open to adopt responsible behaviour when consuming online news.

Thus, the media literate individual is the one who makes informed decisions based on critical thinking, consults high-quality journalistic sources, and promotes media literacy and the credibility of information by verifying the traceability of the information and its authenticity. In the long term, the targeted solutions should refer to media education by interinstitutional collaboration between public authorities, media groups and online platforms.

Conclusions

As we have seen throughout this paper, a strong argument can be made that media literacy is more necessary than ever. In fact, due to this type of hybrid threat, there is an increased interest in developing media literacy, especially for the new generations who collect their information from social networks and other resources online and they must learn to decode what they read and share.

Liberal democracies need to be well prepared in the future to defend themselves against fake news, disinformation and computational propaganda that come from the sphere of hybrid warfare. This time, fake news and mass manipulation will be extremely difficult to control.

Regarding the role of of the ministries of education, they all must insert media education into curriculum pursued at a range of disciplines, from language, social sciences and humanities areas of communication especially since new technologies have significant

advantages: trainees can search for information that complements the ideas provided by the teacher, they all can collaborate openly with other learners, create and share content.

Considering the fact that it is much simpler and less costly to manipulate population rather than militarily and economically conquer a territory, the new approaches to the process of education are needed. New technologies should also be seen as tools in the educational process to be used in order to develop critical thinking and other skills. The effects of fake news are still a matter of debate, but it cannot be denied that these issues have very direct political consequences, as we have seen in several recent events.

Finally, more than ever, it is necessary to empower citizens and facilitate the acquisition of media skills necessary to access, understand, analyse, evaluate and produce content and to distinguish between real and false news. And this has to be done by betting on the benefits of media literacy, with a civic sense that reinforces democracy by building an informed citizenship that can decide freely. It is everyone's responsibility to fight against the manipulation, propaganda and fake news.

References:

1. Blanco, A. V., Nuere, C. O., & Martín, F. B. (2013). The promotion of digital competence for participation and access to digital culture. In *Rethinking Education: Empowering Individuals with the Appropriate Educational Tools, Skills and Competencies, for their Active Cultural, Political and Economic Participation in Society in Europe and Beyond.* Access to the Culture Platform. Retrieved from http://www.houseforculture.eu/upload/Docs%20ACP/ACP 2013WebVersionFull.pdf.

2. Browne, M. N., & Keely, S. M. (2007). *Asking the right questions: a guide to critical thinking* (8th ed.). New Jersey: Pearson Prentice Hall.

3. Celot, P. (2018, March 20). *Why is Media Education Critical in Today's Attention Economy?* Retrieved from www.wise-qatar.org: https:// www.wise-qatar.org/why-media-education-critical-today-attention-economy-paolo-celot/.

4. Digital Single Market. (n.d.). *europa.eu*. Retrieved from https:// ec.europa.eu/digital-single-market/en/media-literacy.

5. Facione, P. A. (1992). *Critical Thinking: What It Is and Why It Counts: A Resource paper.* Retrieved from http://www.student.uwa.edu.au/mwg-internal/de5fs23hu73ds/progress?id=yTaHig48w9pB-Tn4WDkicenF0STu8n4MpufCcsHka8

6. Gallagher, K., J.D., Magid, L., & Ed.D. (2017). *Media literacy&Fake News.* Connect Saftey&Yale center for Emotional Intelligence. Retrieved from https://www.connectsafely.org/mwg-internal/de5fs23hu73ds/progress?id=bPESmAjB733EeyVd-tUrn7rGGMTK1pGih_mciF0DYps

7. Georgiadou, E., Rahanu, H., Siakas, K., McGuinness, C., Edwards, J. A., Hill, V., . . . Knezevic, R. (2018). Fake News and Critical Thinking in Information Evaluation. *Western Balkan Information Literacy Conference*, (p. 3). Bihac.

8. Hobs, R. (2010). *Digital and Media Literacy: A Plan of Action.* Aspen Institute. Retrieved from https://assets.aspeninstitute.org/content/uploads/2010/11/Digital_and_Media_Literacy.pdf.

9. Hobs, R. (2011). *Digital and Media Literacy: Connecting Culture and Classroom.* SAGE.

10. Holmes, M. M. (2018). Media Literacy and Fake News in the Social Studies. *Social Education;nr82(2)*, 91-95.

11. *National Association for Media Literacy and Education*. (n.d.). Retrieved March 14, 2019, from https://namle.net/publications/media-literacy-definitions/.

12. P.Mihailidis. (2018, March 22). *Fake News: Is Media Literacy a Solution?* Retrieved March 14, 2019, from WISE ed.review: http://www.wise-qatar.org/fake-news-media-literacy-solution-paul-mihailidis

13. Paul, R., & Elder, L. (1997). Retrieved from The Foundation for Critical Thinking: https://www.criticalthinking.org/pages/socratic-teaching/606

14. S.Messing, & Westwood, S. J. (2014). Selective Exposure in the age of social media: Endorsements trump partisan source affiliation when selecting news online. *Communication Research*, 41(8), 1042-1063.

15. Swertz, C. (2016). Game Media Literacy. Retrieved from https://homepage.univie.ac.at/christian.swertz/texte/2017_01_GameMediaLiteracy/GameMediaLiteracy.pdf.

16. *The Foundation for Critical Thinking*. (n.d.). Retrieved from http://www.criticalthinking.org/pages/our-conception-of-critical-thinking/411

17. The Knight Commission. (2009). *Information Communities: Sustaining Democracy in the Digital Age.* Aspen Institute. Retrieved from https://assets.aspeninstitute.org/content/uploads/files/content/docs/pubs/Informing_Communities_Sustaining_Democracy_in_the_Digital_Age.pdf.

18. Vosoughi, S., Roy, D., & Aral, S. (2018). The Spread of True and False News Online. *Science*, 1146–51. Retrieved from http://ide.mit.edu/sites/default/files/publications/2017%20IDE%20Research%20Brief%20False%20News.pdf.

19. Wardle, & Derakhshan. (2017). *Information Disorder Toward an interdisciplinary framework for research and policymaking.* Council of Europe.

20. Wineburg, S., & McGre, S. (2018). Lateral Reading and the Nature of Expertise:. Retrieved from https://stacks.stanford.edu/mwg-internal/de5fs23hu73ds/progress?id=sSBpTjrcufVT0hycujXd1LAjokfKnKkHglG1VDjl3kg,&dl.

21. Woolley, S., & Howard, P. (2016). Social media, revolution, and the rise of the political bot. In P. S. P. Robinson, *Routledge handbook of media, conflict, and security* (pp. 282–292). New York: Routledge.

TERRORISM IN THE FUTURE: STRATEGIES AND METHODS TO ELIMINATE, PREVENT AND MANAGE ATTACKS OF THE NEW TERRORISM

Sabrina MAGRIS[*], Martina GRASSI[*]

Abstract

The phenomenon of internal nationalisms with international infiltrations, which is rising again, is a global one – experienced from Europe to America – not to be overlooked. It is a phenomenon that leads to domestic terrorist attacks and its characteristics distinguished it from other types of terroristic attacks that are of a non-Islamic matrix, thus adducing to a higher risk to take place than during the past.

This is the motive that drives young people that – as already reported by some Intelligence agencies – even if they don't have a concrete knowledge of the historical events that have occurred in the past or about the various ideologies developed over time, to follow the ideologies of these individuals. –Some of the analysed solutions concern obtaining consent through the mass management and handling techniques used in Psyops Operations for the construction of consent to leaders. In the training of leaders, when communicating to the mass, it must be kept in mind that one cannot simply refuse requests without giving justifications, the reasons why decisions are made must be explained to the population so they can be well understood so as to limit or to eliminate the dissent. The senseless denial must never be used, and the masses consent and consent to leaders must be built by using more groups of people, included those who dissent, so to convey dissent. Therefore there must be created dissenting groups to the leaders that are credible and vehicular to all those who have opposite opinions than the leader, so that to be able to convey and to manage potential opponents in the best way.

Keywords: *terrorism, domestic attack, intelligence, aggregator, strategic communication*.

[*] President of École Universitaire Internationale, Director of Research École Universitaire Internationale Rome – Italy, president@ecoleuniversitaire internationale.net.

[*] Head of International Activities, Fellow Researcher, École Universitaire Internationale Rome – Italy, ia@ecoleuniversitaireinternationale.net.

Introduction

This paper addressed the rise of the evolution of Internal Political Terrorism, a phenomenon that is spreading all over Europe and that had already caused several terrorist attacks. This study will present specific counteractions tailored for this type of internal terrorism with immediate, mid and long-term actions. It will present directives designed specifically for the education and training methods for intelligence practitioners. It will clarify the process by which this type of terrorism started to take hold by exploiting the growing disappointment of the population towards politics and also by using the perpetual search of the youth for an identity. The study will analyse the different figures and contexts in which this internal terrorism has set upon and the characteristics of the people involved, through the analysis of different attacks. It will specifically address how the attacks have been conducted with the use of old terrorist group techniques updated to the modern context and how Intelligence counteraction can be used by basing its strategy on old techniques and new neuro-structured approaches.

Ultimately, this paper offers a structured analysis of this new phenomenon, regarding the territories involved and explaining the methods used by the terrorists to attract as many subjects as possible. Every terrorist action, weather it originates from issues concerning Islam, or draft of eco-terrorism, domestic terrorism, or politically oriented one, it causes damage to the State where it occurs, even if it does not have the effect foreseen by the terrorists. The effects can thus have various forms: they can range from image detriment to political damage, from creating terror among the mass, to implementing the annoyance of fanatics and individuals who have no belief system but whose sole purpose is to unleash their aggression by emulating each other. A clear example could be those individuals who started throwing stones to vehicles from overpasses, simply because they saw someone else doing it but without a real motivation.

Terrorism is communication: avalanche effect

The preferred means by terrorists to send their messages to an audience is communication, as the only one capable of guaranteeing results on a large scale. A terroristic action, if not highlighted by the media, does not have the desired impact so it can be considerate inexistent. The only way population can get to know about terroristic attacks is through the information spread by the press and television. Every day around the world terroristic attacks happen although populations belonging to States and continents different than the ones where those acts occur rarely get to know about those news. The more the media emphasizes a terrorist attack, the more likely it is that the news of the event reach a large number of people, so the populations becomes aware of it. Great media attention for terrorists attacks means that the terrorists in question are being placed in a position of relevance at the time when the attacks occur, and they and their cause become like a light for their supporters, without taking into consideration the real victims and damages of attacks.

As stated before, it is to affirm that there is a great difference in media emphasis between the terrorist attacks that had a limited number of victims and damages and those where, instead, the numbers are much more substantial, so to underline the importance that newspapers and TV give to one attack rather than to another one. Information management can create panic and anxiety among the people who get to know about terrorist acts, so it is fair to say that if a terrorist attack is not planned into an area covered by important television and newspapers, it does not exist. Statistically, average Europeans do not remember a news learned more than three days before; they do not read or listen news coming from an information source different than the ones from their own State and into their native language. This fact allows us to be able to identify possible terrorist groups structured for individual attacks precisely by virtue of the choice of the place where the objective is located and to whom the objective is; this is possible because the final purpose of the structure will be the one to have a media prominence rather than creating significant damage to people and things. A clear example of this

avalanche effect is the *Bataclan* attack happened in November 2015 in Paris, France.

After the *Bataclan* attack, France had to face the various effects of the attack. There have been numerous deaths, major economic losses and very high expenses to repair both direct and indirect damages caused by the attack, as well as to improve safety. According to the Institute for Economics and Peace (2015) the terrorists' budget available for committing the attack was around 18.000 Euros. The economic consequences for the entire community have been much higher. But the internal effects are not the only ones caused right after the attack: the attack had also important consequences abroad, economically speaking, that affected other states, including Italy. The terrorists who committed the attack, then stated that they had not foreseen such an avalanche effect abroad. (Proceedings of the trial of Salah Abdeslam, defendant of the terrorist acts in Paris, November 13th, 2015)

As anticipated, as a consequence of the *Bataclan* attack in Paris, Italy suffered significant economic losses. Shortly after this terrorist attack occurred, in Italy, precisely in Rome, there was the Catholic Jubilee of Mercy (from December 8th 2015 to November 20th 2016), a very important event for the Catholic Church, and therefore for the whole Catholic world: it is a year during which every religious has the opportunity to receive the total cancellation of the penalties provided for their sins, which necessarily involves crossing the threshold of at least one Holy Door. It is an event normally held every 25 years, although the Pope may decide to hold an extraordinary Jubilee – as done by Pope Francis in 2015. For the Jubilee, the City of Rome, and all Italy, were waiting for a very high number of pilgrims and tourists, people who had booked hotel rooms, vacation houses and transportation. As a result of the attack, most people cancelled their reservations and plans because they were terrorized by the possible advent of a new terrorist attack. This caused tremendous economic loss for the entire State and for the City of Rome, since restaurants, transportation, hotels and all kinds of productive activities suffered great loss both due to the fact that the reservations were cancelled and both for the large investments that many had made in order to better

accommodate pilgrims and tourists that, in the end, no longer arrived. This impact was publicly reported by the Rome Chamber of Commerce underlining the fact that no terroristic attack took place in Italy. (Rome Chamber of Commerce, 2016).

Internal Political Terrorism and transversal actors

In the past years the discourse has been focused on Islamic terrorism. Today Internal Political Terrorism (IPT) is on the rise. This fact is caused by the current distrust of the population towards the political class and decision makers, and this is an occurrence that happens in several European States. This is a current threat, as considering the fact that various internal terrorism attacks have already taken place in several States, forcing intelligence to consider and to counteract this type of terrorism that works with transversal actors.

For example, a specific terrorist attack took place in Italy in August 2018, in the city of Treviso. It was a bomb attack deposited and detonated at the headquarters of the Political Party "Lega". In this case, with the incrimination for terrorism, a Spanish anarchist and an Italian were arrested a year later. Thus, in this and others attacks, emerges that there is a transversal line of collaboration in internal terrorism that links the various European terrorist groups to each other in order to carry out attacks, which was typical of the 70s and the 80s as simply demonstrated in the various Court processes and investigations. From these arrests it emerges the age difference between the terrorist subjects, their different nationalities and, contextually the different political opinions which converge, in spite of it, in carrying out the specific terrorist act. (Il Fatto Quotidiano, May 2019/ ANSA, August 2019, Attack on the headquarters of Lega of Treviso)

The transversal aspect refers to the fact that the Internal Political Terrorism involves and lures individuals who are very diverse from one another. It is transversal with regard to their age, social class and ideology. It becomes extremely easy to external sources to offer to youth many identity hints regarding the construction of an identity, considering the problems that young people have in building one that can be able to support their behaviour and their life choices in a balanced way. Today these youth rarely have an ideology.

As *World Health Organization* (WHO) data state, in the last twenty years young people have undergone changes: these are not only psychological changes but also physiological changes. Physiological changes have occurred in their brains, in fact it has been proven that the white matter in their brains is less than twenty percent thicker than the one of young people of the same age ten years ago. This is the cause of the decrease in the number of neurons and of neuronal connections present in their brains.

It is important to emphasize the way in which the physiological, psychological and social changes that have taken place outside and inside young people today have led to the increase of micro pathologies caused by excessive use of mobile phones, tablets and technological devices. Among the micro pathologies of this kind that have been observed among young people, there are FOMO, Sensorial Distortion, False Perception and others, all pathologies that render youth easier to manipulate. (JWT-J, 2012; RSPH, 2017; Loppi, 2018)

The diminished neuronal connections mean that the construction of thought, one's own identity, as well as the perception of the self are discordant from the real self and that there is a simple, less elaborate and less nuanced possibility of thinking.

As pointed out above, these social, physiological and psychological changes in young people have influenced their way of acting and making decisions and have rendered youth more easily attracted by this internal terrorism that offer them the possibility to quickly have an identity, that identity they seem not able to create on their own.

Although they are, therefore, in search of an identity and of an ideology, they aim to acquire them by putting as little effort as possible. It is easier to follow an ideology and to be part of a group placed in their own territory and to follow who make use of their native language, without the need to move abroad or to learn a new language or new religion in order to be able to follow the ideology.

Youth are seeking for an identity but they do not want to work for it, to put themselves on the line. It is in this type of internal terrorism that youth find their certainties, security and the ordinary things to which they are used to, as their lack of identity and its

research leads them into a circle of "indifferent" social polarization. This type of terrorism thus becomes alluring not only because it gives to youth the opportunity to have an identity, but also because, at the same time, it allows them to unleash the repressed aggression that has formed within them with no apparent reason, their Apathetic Aggressiveness. The term Apathetic Aggressiveness refers to all those extremely aggressive behaviours that have no motivation, such as those youth who kill and torture a peer and when asked the reason s/he did it, s/he answers *I don't know, I wanted to see how someone dies* (École Universitaire Internationale, 2016).

In the search for their identity, young people are attracted by ideologies that very often they do not deeply understand and that thus exchange for their own identity. In order to reach with certainty the conclusion that a certain ideology is one's ideology, the process contemplates knowledge of the historical facts occurred over time, as well as of the different existing ideologies. Young people are often unaware of it and are not even interested in getting to know them. It is in this confusion that they grab themselves to false tailored ideologies, trying to base their identity on them, and it is still because of this confusion that they are easily attracted to terrorist groups that claim to be able to offer them the desired identity and ideology they were looking for, although it is a false identity and just a way to unleash their suppressed aggression. They roam as wounded animal with no identity and full of resentment.

If in the past years the Islamic State (ISIS) attracted many youth thanks to this series of characteristics (due to its massive use of propaganda), this current internal terrorism has the capability to attract not only youth, but also adults. They can be a source of hope for those adults who have been disappointed by political parties and by politics at large. They had and they still have an ideology that has been betrayed by the same people, by those politicians and political parties that should have protected them and supported their ideologies. Thanks to its transversal characteristics, the Internal Political Terrorism is able to attract completely different individuals from one another.

It has been proved how ISIS made specific videos in order to attract young people of various nationalities, by editing them with television commercials and videogames modes. The music, the colours and the image sequences were always made by copying the Hollywood style and characterizing them with stories in the languages in which the movie would have been widespread. BBC has made a specific search for a documentary aired in 2016. Islamic terrorism has a broad culture, something that has not been seen in terrorists of the last decade. The broad culture and the knowledge in various themes make the figures of these subjects fascinating, they are seen as anti-state figure, and contextually in the imaginary seen as liberators, as some Robin Hoods who struggles to subvert a totalitarian power. With this reading it is easy to ensnare young people, like those highlighted above, by a subject who has carried out terrorist acts (2015, BBC).

Speaking about the adults, in the climate of political disbelieve – which is affecting various States – the mentioned adults are easily attracted by these Internal Political terroristic groups that provide them a way to avenge their betrayed ideology and to fight for them by any necessary means. These adults, who find no alternative among the political arena, can be lured by internal terroristic groups.

An important fact that should also be highlighted is the different methodology used by the two types of terrorists that does not only depend on social and psychological aspects. The two methodologies are different not only because of the kind of preparation and methods of performance, approach to planning and to carrying out the attack, but there are also many differences in the aspect that should be emphasized most of all: the modification of the diminished neuronal connections among subjects aged less than 45 years old, as already proven by science in different occasions (WHO).

Terroristic groups with old schemes in today's context

These new internal terroristic groups act following old schemes and military tactics already used by the terroristic groups that had acted in Europe in the 70s and 80s updated to the today's context. These are terroristic groups such as BR Red Brigades, ETA Euskadi Ta Askatasuna – Basque Homeland and Liberty, IRA Irish Republican

Army, NAR Armed Revolutionary Nuclei. The union between updated old military tactics and the current social context describes the characteristics of this current internal political terrorism. This union is particularly evident in the mentioned recent attack committed in Treviso, the north of Italy (2018) and in the recent New Zealand attack. On March 15th 2019 at Christchurch in New Zealand a 28-year-old man attacked two mosques with rifles and guns killing 50 people (The Guardian, 2019).

Both the way the attacker carried out the attack and the way he trained for the attack resemble old techniques that belong to specific geographical territories. As the attacker stated, he has been trained in ex-Yugoslavia territories by people familiar with guerrilla techniques used in those territories at the time of the war of Former Yugoslavia.

The attacker, equipped with rifles, guns and explosive tanks ready to use (typical modality of Sarajevo attacks) entered the mosque using military tactics and started shooting at the people present. On the rifles and gun there were written on names of people he considered as model to follow as they committed terrorist attacks with similar motives. From the video he posted on-line, it is visible that in the trunk of his car there were other rifles, guns and explosive tanks ready to be used. The explosive tank is an important detail since using explosive tanks in order to turn cars into bombs is an old technique developed in the Balkan area during the Balkan conflict, as well as using another explosion after the attack, when the first responders arrive on the site, in order to create more victims and damages. Many have overlooked this detail, even in the analysis of the video and of the images of the car trunk the attention has been drawn on the dark rifles with white writing on, without taking into consideration the tanks right next to them. This is an important detail in order to start the investigation on every individuals involved. In fact, the attacker had previously travelled across several countries including Montenegro, Serbia, Bulgaria, Turkey, Pakistan and others. However, when taking into account the subject that committed the attack, there are many incongruities that come to light.

The attacker is an Australian man who stated he wanted to liberate his state from *'those who went there stealing jobs from the*

native population', but he committed the attack in New Zealand and not in his own country. The writing on his rifles refers to individuals he thinks to be model who share his same beliefs; on a rifle there is written the name of Traini Luca – an Italian man who shoot against black people in the streets in Italy without deaths in February 2018. However, Traini, after his arrest, rejected his racial motive saying that he committed a mistake and was glad nobody died. This shows the little knowledge the New Zealand attacker had of facts, and consequently shows a weak ideology based on false beliefs rather than real motives. The above demonstrates the statements made so far applied to a real case. The terrorist was born in Australia, he lived in Australia and carried out the attack in New Zealand declaring that he wanted to free his State from the invaders. This definitely shows a confused situation in the terrorist's mind. The New Zealand is not his state, he is a foreign subject in New Zealand, and he himself would be one who steals the job of the New Zealanders. It takes its cue from past and recent historical situations that have nothing specific related to terrorist acts aimed at driving out invaders. The most striking case is to cite the Italian Luca Traini who declared himself, to the Italian judges of not being a terrorist, of having nothing against black people and non-Italians, that he made the gesture in a particular psychological moment of his life apologizing to have injured people and making himself available to pay damages. We therefore have a clear picture of a terrorist, the Australian, who reflects the characteristics highlighted by the studies we carried out (École Universitaire Internationale, 2015, 2016, 2018).

As already mentioned before, on August 15th 2018 Italy has suffered an internal political terrorist attack that took place in the city of Treviso. Two explosive devices, one of which exploded: one was placed up on the stairs located inside the building, and the second one in front of the external door of the local head quarter of a right-wing political party, Lega. This modality indicates that the person who positioned the explosive devices knew what he was doing and how to place the devices in order to cause more victims and damages as possible. The explosive device placed in front of the external door was aimed to attract the attention while the second one up on the stair was aimed to cause the massacre.

On October 13th 2018 Italy suffered another terrorist attack that took place in a north region of the State, in Trento. The attack was accomplished by placing explosives. The attack resembled the same old tactics and schemes used by 70s and 80s terrorist groups, and that has been committed in the same places. The terroristic group placed two explosive devices in front of the local head quarter of the same political party, one of which exploded without causing victims; they damaged radio-transmitting trellis blocking radio communication and they also damaged university laboratories.

Another thing similar to old terrorist groups is the fact that the attackers lived together in a house. On February 18, 2018, Italian Police and Italian Counter-terrorism arrested seven anarcho-insurrectionists, responsible for the attacks in northern Italy. Also in this case we are talking about Italian subjects, including several young people and two men of about 50 years old. The group is accused of at least three attacks plus others being investigated, which have always been carried out with bombs in recent years. (AGI, February 2019, Terrorism: anarchic-insurrectionist cell in Trento, 7 arrests)

As anticipated above, the way these two attacks were conducted resembles techniques and tactics used in the Former Yugoslavia territories during the conflict. In both cases there have been used a technique that took hold in Sarajevo during the conflict, and then used in different places in the world. A first explosive device exploded in order to create injuries and damage and rush rescuers and onlookers, to then explode manually, by pressure, or with a remote control a second explosive charge much more powerful, in order to make a massacre.

In an objective Intelligence analysis individuals that have been deployed in these territories should be monitored as they are looking for a positioning. Since they had lived a past that saw them as protagonists in these war situations, and having them seen particularly heavy situations for the human psyche, once they returned to their own countries they found themselves no longer having the importance they had during the conflict. However, since they have learned the only profession of combat, they look forward to re-establish their knowledge and at the same time are seeing a social position re-allocated. Studies

on aggression and on the psychic state of veterans have been carried out by the US government and repeatedly cited by various studies and sources, so much so that since the 2000s the US State Department had issued specific indications that veterans who commit criminal offenses against things and people should not be put in jail with common subjects. This because of their specific knowledge in the use of combat weapons and fight methods (US Bureau of Justice Statistics, 2015).

From an investigative point of view, Intelligence professionals should be trained in putting together information into an interdisciplinary way. It must be taken into consideration that this type of attacks are committed by groups of individuals – rather than a random single individual such as attacks committed by infatuated – (École Universitaire Internationale, 2018) so detecting them it's easier because of the greater exchange of information between the group members, which means higher possibility of committing error and leaking information. In addition, a high number of people means a greater probability to identify the weakest link. As this type of terrorism is an internal terrorism, the group members will talk the same language (most probably the one of the State they live in) and it will be necessary for the practitioner being able to understand not only the language spoke into that territory, but also its dialects and its idioms. Compared to the old internal terrorism groups, it is easier and common nowadays having members of the group that speak new languages. For instance, non-native members that speak other languages, and that mix their own language with the State language: a mix of terms of the different languages that leads to the formation of new mixed languages or new idioms that are hard to understand to those who are not part of the group (i.e. a person originally from Ukraine that lives in Italy and speaks both Italian and Ukrainian, mixing the two and creating mixed terms and way of saying).

For the purpose of monitoring these groups and gathering information is necessary the use of old techniques applied to the new modern context. Although using wiretap and transmitters with a lone wolf or an infatuated was harder (because of the little or no exchange of information), they become useful with these groups, as the "chiacchiericcio" technique becomes helpful again. The "chiacchiericcio"

technique, in fact, monitors the intensity of information. For instance if in the group there is an exchange of information between the members which then suddenly ends, to then resume again among all the members or even among only some of them, there is a high probability that an event is about to happen. In addition, when having a group, Humint operations become useful. Although having more individuals to monitor has a higher cost, the quality of the information gathered is more valuable and accurate.

Although these techniques are dated, their use updated to the current context become invaluable. To achieve this, senior professionals need to teach young professionals the old techniques and tactics so that young professionals are able to implement them in the current context by updating them. This exchange will ensure that intelligence can upgrade its *modus operandi* and therefore its results, avoiding the gap that it has experienced in the last decade where there was not kind of exchange of information between senior professional and the young ones, with the result of obtaining unprepared young practitioners replacing *tout court* old professionals and so losing their experience.

This exchange of information is able to make intelligence analysis more efficient and precise: it will ensure that professionals are able to correlate information regarding how the attack was committed to the ones about who committed it. Recognizing a certain type of *modus operandi* of the attackers, therefore understanding where they have been trained and, therefore, being able to correlate it to a specific geographical area of belonging, allows to delimit the area of investigation and to earlier identify the individual. Therefore, the ability of recognizing this type of detail is essential for conducting the investigation in an appropriate manner. For instance, a person trained in the UK, or someone deployed, acts differently from a person trained in Russia; at the same time the way a person from the Balkans slits throat is different from the way someone from Latin America would do it, so a person from Egypt tortures differently than someone from Venezuela. Knowing these aspects and being able to recognize them, will enable to forecast the type of the next attack, where it will take place and to whom it will be directed, and to know the way the attackers have been trained.

Though all this becomes possible only if senior practitioners will share their information with young practitioners: only those who have worked in certain scenarios and during a certain time possess this type of information and detail.

This is all possible because the human brain works by creating repetitive models, and it survives using the same repetitive models and making the individual repeating the same schemes. This is the reason why practitioners must have a flexible and non-repetitive brain: it would be able to get out the repetitive schemes and then successfully detect threats and early counter act them. In order to be able to render it this way, the practitioners' brain could be trained with the *Double Imprinting* technique, for the purpose of having a better performance of the brain in analysis, speed and resolution of the problems. (École Universitaire Internationale, 2016)

During the intelligence training, including subjects that address the way thought is formed is also important, not only from a strategic and political point of view, but also from a neuropsychological one, addressing how brain works and how neurons can affect decisions and the creating of thoughts.

When analysing this type of current internal terrorist attacks, different peculiar characteristics came to light. The group members greatly differ in age, geographical origin and cultural level and this highlights the role of a figure that is crucial for these attacks: the Aggregator.

The role of the Aggregator

The aggregator is an individual that attract members and aggregate them into the group. S/he is not a member of the group. S/he provides both the tailored ideology for the youth seeking an identity and the chance to avenge the betrayed ideology of those disappointed adults. S/he has likely being involved in subversive actions or has been a supporter, s/he might have a military training, s/he might have been in prison and s/he can be that model, that beacon that attracts others. s/he has experience, knowledge, connections and appeal. The aggregator is empathic; s/he has a halo of credibility and s/he is able to communicate it.

This type of figure was not common in the Islamic terrorism that committed the terroristic attacks in Europe in the past years. The only case in which the aggregator was presented is related to the terrorist attack of August 17th 2017 in Barcelona, Spain. In this case the aggregator was a men around forty years old, he was the football coach of the youth that committed the attacks on *La rambla* (Centro Nacional de Inteligencia, 2018). He persuaded those youth into committing the attack. In this case the aggregator was the real motive behind the attack. The bombers were all young soccer players of the team coached by the man, the aggregator indeed. The aggregator gave his own motivations to the young people who, in order to avoid the exclusion from the team, carried out together this terrorist attack. The young people did not have a marked religious identity and they were substantially different subjects from one another. The only magnet was precisely the aggregator who was also the one who studied and prepared the attack. However, he did not take part to it, letting the young soccer players carrying out the attack. The aggregator, in this case an adult man, felt psychologically important since he was the head of a team of young terrorists that put into place what he thought and named.

The aggregator does not take part in the terroristic attacks. Considering the scenario that has arisen, intelligence should use different and new techniques when dealing with this phenomenon. This new internal political terrorism raised because of people's disappointment towards the political class and the actions of the decision makers.

The first action to implement is speaking to the population. It consists in explaining to the population why the decision makers decide for an action, by using simple terms that are effective and able to include the whole population. In order to ensure the security and the stability of the State, the Intelligence should indicate to the decision makers which are the most effective solutions to be taken. Economic Intelligence, Operational Intelligence and Strategic Intelligence must therefore work in order to ensure that politician's communications become more widely disclosed and that are simple and clear, so to have the support of the population and to obtain the result that population

itself communicates anomalies or facts to the police and Intelligence, thus building a social information fabric: so to make territory, companies and the State itself safer, and it happens not by the creation of a state of deletion, but through a state of collaboration between free citizens that are made aware of the fact that reporting things to the police is not bad and that it can serve to avoid attacks and facts in general that could create problems for the state. So the bottom line is explaining that the whole is, and must be created for the progress and the good of the state. This is a method of communication that is strategic and effective (Bellomo, 2015).

For instance, explaining the reasons why there is an increase in alcohol taxes. The decision maker should explain to the population that the rising of price has the purpose of determining a decrease in the numbers of the buyers, it will so head the rise of competitors that will determine a higher quality of products and also the fact that the money gathered will be used to improve the cure of diseases linked to alcohol. The decision maker should established a period of time, i.e. six months, in within which to publish the collected data so to create within the population, in a period of time of 24 months, credibility of his decisions showing he does what he promised. If the tax increase should not have the expected result, the decision maker should stop the project without trying to justify himself or his decisions. The first phase is creating a true credibility of the decision makers.

In order to do so the decision maker's education should be oriented towards national security. They should be educated and trained in leader communication and strategic communication, while intelligence practitioners should be also trained in neuro-structured approach techniques. Speaking in a strategic manner to the population will also lead to the result that even those who initially had doubts will flow into the majority group, thus homologating the group in favour of the decision makers. It is known that the population does not question a high salary if it witness positive results. The questioning is the result of the population disappointment towards the institutions and decision makers.

The second action is the approaching phase in counter terrorism activities. It must be activated among the youth from 14 years old. It must provide those different hints and more options in order to let the youth free to find the option that best suits them.

Youth need to be stimulated, they can be approached by using their own language. It is important for young people to find a way to unload their energy and to express themselves and having more ways and hints among which they can choose, will lead to higher probably that they will choose one of the ways offered by the community instead of being attracted by the terrorist world, giving them the opportunity not to be attracted by wrong models and by the aggregator.

Young people are not looking for a friend but rather for someone that can indicate them a path, someone to trust. These actions are based on the behaviour of the mass and of the single individual who works simultaneously on both of them.

There are three different strategies that can be implemented in order to decrease the aggregator's appeal. One of them consists of a tailored action aimed at managing the acute intervention through a neural inhibition of the individual. For instance, recent studies have discovered a new inhibitor neuron located in an external part of cerebral cortex, called Rosehip (Eszter et al, 2018). With the use of the inhibitory action of the neuron it is possible to block the individual from continuing the action s/he is committing, thus stopping him during the action or interacting to him so that action will be totally inhibited. The second strategy consists in using the normal methodologies of communication that can be used to move away the individual from the aggregator. The first strategy is intended to be used during the action (immediate strategy), while the second strategy is intended to be used outside the action (mid-term and long-term strategy). The third strategy consists in using a fake aggregator (cover action) that works to separate the group rather than aggregate them.

Conclusions

Concluding, the current internal political terrorism is on the rise. The individuals that have committed attacks differ greatly for age, social class, geographical origin and cultural level. They usually act

within a group: the individual is attracted by the aggregator who is not a part of the group but is the one who aggregates it. The groups use techniques and schemes used by past terrorist groups updating them to the new context of action.

As in the past, also the current internal terrorism has international ties. For instance, ISIS terrorists are likely to flow into this type of terrorism: since ISIS has been defeated, they have no longer a place in it. Indeed, it is unlikely for them to try to merge in Al Qaeda. Al Qaeda is a structured terroristic group that respect the Quran, contrary to ISIS that does not respect the Quran as its terrorists do not know the Quran. ISIS terrorists cite a modified Quran, in fact the same Quran that is distributed by ISIS is not recognized by Islamic communities as it is modified in several parts and does not respect the sacred scripture. In actual fact they committed terrorist attacks also in the sacred months, the ones during which Prophet Mohammed stated that no kind of violence is allowed, and whomever disobey this precept will be automatically condemned. ISIS terrorists are more likely to try to recycle themselves by becoming the soldiers of those who pay them or to flow into this internal terrorism where they could have a higher consideration and a role as having them already fought. As mentioned, young or adults that have not a clear creeds, beliefs or identity can became part of a group (terrorist group) not following an ideology but just to be part of "something".

Furthermore, the future internal terroristic attacks will have a military oriented structure along with an excessive cruelty. The future attacks will be more precise, more structured, more violent and committed with greater cruelty. It goes without saying that intelligence should be trained with the new and advanced techniques in order to be ready to effectively counteract this phenomenon.

References:

1. AGI, (February 2019), *Terrorism: anarchic-insurrectionist cell in Trento, 7 arrests*, retrieved from https://www.agi.it/cronaca/terrorismo_cellula_anarco_insurrezionalista_arresti_trento-5022077/news/2019-02-19/.

2. ANSA, (August 2019), *Attack on the Headquarter of Lega of Treviso, for the Prosecutor's office it is terrorism*, retrieved from http://www.ansa.it/veneto/notizie/2018/08/16/treviso-ordigno-esplode-allesterno-della-sede-della-lega_36ae793d-f139-48a4-abc3-a2edd163d981.html.

3. BBC documentary, (2015), *Examining Islamic State's social media strategy and what can be done to combat it*.

4. Bellomo D., (2015), *Advanced Security*, Italy.

5. Centro Nacional de Inteligencia report, Spain, 2018.

6. Eszter et al, (2018), *Transcriptomic and morphophysiological evidence for a specialized human cortical GABAergic cell type*, Nature neuroscience.

7. Global Terrorism Index 2015 Report, Institute for Economics & Peace.

8. Grassi M., (2016), *Apatetich Aggressiveness*, EuiEdizioni.

9. Il Fatto Quotidiano, (May 2019), *Treviso, had put a bomb in front of the headquarters of the League: stopped Spanish anarcho-insurrectionist that was already a fugitive*, retrieved from https://www.ilfattoquotidiano.it/2019/05/28/treviso-aveva-messo-una-bomba-davanti-alla-sede-della-lega-fermato-un-uomo-vicino-allarea-anarchico-insurrezionalista/5213956/.

10. JWT Intelligence report, (2012), *Fear of missing out*.

11. Loppi A., (2018), *L`isola che non c`è. La vita su Instagram*.

12. Magris S., (2015, 2016, 2018), *Studi sul terrorismo*, Quaderno 1, 2, 3 École Universitaire Internationale.

13. Magris S., Grassi M., Di Gioia P., (2018), *Intelligence and counterterrorism: the meaning of words is the right tool to make an efficient analysis when the threat is hybrid.*

14. Magris S., Grassi M., Fanti F., (2016), *Psychoanalysis between role playing and changing identity: double- imprinting. Psycho-anthropological training of the intelligence officers employed in international complex scenarios*.

15. *Rome Chamber of Commerce report*, 2016.

16. Royal Society for Public Health (RSPH), (2017), *#StatusOfMind report Social media and young people's mental health and wellbeing*.

17. US Bureau of Justice Statistics, 2015.

18. *The Guardian*, (April, 2019), Christchurch shooting suspect will face 50 murder charges, say New Zealand police, retrieved from https://www.theguardian.com/world/2019/apr/04/christchurch-shooting-suspect-will-face-50-charges-say-new-zealand-police.

CURRENT TRENDS OF CYBER TERRORISM IN THE MIDDLE EAST AND NORTH AFRICA

Florentina-Ștefania NEAGU[*], Anca SAVU[*], Tiberiu TĂNASE[*]

Abstract

The phenomenon of cyber terrorism has grown globally and the states of Middle East and North Africa have not been circumvented, a major cause of the spread of the phenomenon is Internet users' access, so that in North Africa in 2000 the number of Internet users was 710,000 and in 2017 there were 102 million users; this means 45% of the total population of the region. Another factor is legislative shortcomings or even their absence, for many years Tunisia did not have a law on cybercrime instead of using the law on e-commerce. The same thing is happening in Morocco that uses the trade law.

Algeria and Egypt have no cybercrime laws, but publicly announced that then declare the cyberspace domain of national priority. The only states where there is no law on cybercrime, communications regulation or other laws on new technologies are Libya, Syria, Yemen, Iraq, and Kuwait. Attackers' motivations are money-related, infecting devices by sending malware via e-mail, commercial and industrial espionage. The tools they are using include: web app attacks, ransomware, targeted attack, defacement, espionage, insider threat, theft and physical damage, DDos, phishing and malware. Taking into account the political and economic evolutions in the region as well as globally, there is an upward trend in cyber terrorism.

Keywords: *cyber terrorism, dark web, information warfare, intelligence, risks.*

[*] PhD Student, Bucharest University of Economic Studies, Romania, Email: stefanianeagu15@yahoo.com

[*] PhD Student, National Defence University "Carol I", Bucharest, Romania, Email: ancasavu91@yahoo.com

[*] PhD Researcher, Division of the History of Science of the Romanian Committee for History and Philosophy of Science and Technology - CRIFST of the Romanian Academy, Romania, Email: tiberiutanase26@gmail.com

Introduction

Worldwide, the IT industry is experiencing steady growth by employing an increasing number of staff due to the emergence of new types of malware. According to Panda Security, daily, 230,000 new malware attacks are recorded at 39 seconds time interval. Most attacks have taken place within the retail and technology industry, small and medium-sized enterprises, but also against government institutions, because they have access to a high level of personal data but also because large amounts of money can be earned by providing the data decryption key. Attacks targeting companies include phishing, social engineering, bootnet, malware, Hackers' medium time to access a company's servers is 22 minutes (Ziffer, 2019). The main cause of these vulnerabilities in 95% of cases is given by human errors. At the end of 2018, the total cost of cybercrime was over 1 trillion dollars.

The main tools used by hackers

A study conducted by SciDevNet shows that there are 450 million internet users in Africa, which indicates an increase of 9.941% from 2000 and to 2018 with a penetration rate of 35.2%. The high level of Internet connection is accompanied by a high rate of software piracy, especially among African and Middle East countries. Cyber criminals mostly use infected computers fed to pirated software. In 2013, International Data Corporation conducted a study which showed that 33% of global software is counterfeited, valued at $ 114 billion worldwide. The countries with the most affected IT infrastructure were: Libya (92%), Algeria (84%) and Nigeria (82%).

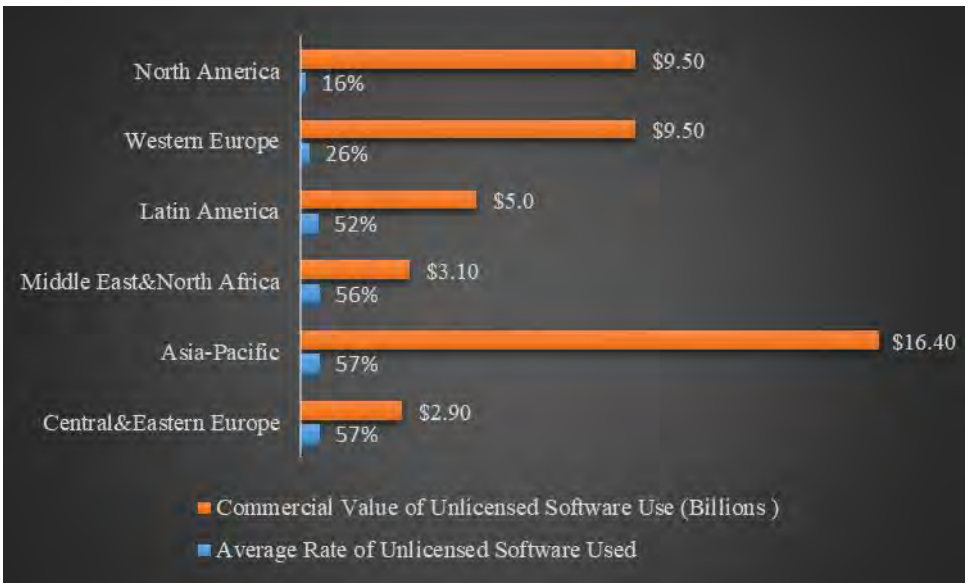
According to estimates made in 2011, the percentage of pirated software in the Middle East and Africa was 58%, while Microsoft estimated software piracy on Kenya's IT market of 78%, which means a loss of $ 120 million. One of the causes that facilitate software piracy is the outdated or outdated operating systems. Counterfeit software and applications can be easily exposed to cyber-attacks. At the level of Africa, about 80% of user computers are infected with malware, viruses, and other programs. The most common tools used by hackers

are key loggers that benefit from encryption and file protection. The value of a key logger is $ 35 and can be easily purchased from Dark Net.(BSA Global Software Survey, 2018)

In figure 1, we can see the commercial value of unlicensed software and the average rate of unlicensed software around the world. The highest commercial value is in Asia-Pacific, North America and Western Europe and the smallest in Central and Eastern Europe and the Middle East and North Africa. The main threat worldwide has proven to be Cryptominers, which have affected 42% of the world's companies, generating $ 2.5 billion. The operating mode of these cryptominers has evolved from Facebook's Messenger, Youtube to Google Play announcements, which infected tens of thousands of websites, personal computers and mobile applications. (BSA Global Software Survey, 2018) Many types of malware have integrated mining capabilities into their operating mode, ransomware, and bank trojans, including Panda and TrickBot, which target not only bank accounts, but also encryption wallets and trading system accounts, adding features of credit theft cryptocurrency in the operating mode.

Cryptominers are also a threat to cloud services that involve data seclusion and information disclosure that stem from low security. Cryptominers target cloud infrastructure to exploit stored data and generate increased revenue for exploiters. In the first six months of 2018, cryptomers targeted two main components of the Docker and Kubernetes systems. One relevant example of attack by cryptominers is the internal cloud servers of the Tesla that have been infected with a Monero cryptomonitor (Check Point, 2018).

Figure 1: The value of Unlicensed Software Globally
(Source: Author's own processing based on BSA Global Software Survey, 2018)



The evolution of cyber terrorism in the Middle East

With the development of information technologies, the threat of cyber-attacks and terrorism has emerged throughout the world, which in turn affects the decline of state and citizens security. Following the tragedy of September 11, the Western society has suffered a fear of terrorism coming from the Middle East. But what we should know is that only certain groups in the Middle East represent a terrorist threat. Undoubtedly, terrorist threats from groups like Al-Qaeda or the Taliban are constant for governments, especially the United States.

However, the evolution of technology and the Internet, as well as the embrace of terrorist groups of this trend, makes governments confront another type of terrorism, namely cyber terrorism. Cyber terrorism has expanded so much and quickly that it has become the first issue on the US national security agenda (Gielten, 2013). The danger of cyber-terrorism in the Middle East started when the former Al-Qaeda leader began using the internet to upload videos during

certain speeches. In the present, the Islamic State collects all the Middle East titles.

Different from Al-Qaeda, ISIS is more of a threat to countries around. With the evolution of the cyber war, the term "e-jihad" also emerged, which essentially means "electronic jihad". ISIS uses cyber space to preach Islamic ideas, spread ideologies or disrupt Israeli sites (Tereshchenko, 2013). The adoption of new technologies by terrorist groups helps them in recruiting staff, highlighting goals, spreading fear, and raising funds. Their purpose is to use the cyber platform to penetrate target networks easily, with low detection and low cost (McFarlin, 2014).

The Middle East region is an easy target for cyber-attacks, mainly due to the lack or low level of awareness of the threats posed by Internet users and the lack of legal regulations. The element generated by the number of attacks is the presence of numerous political, economic and social conflicts, but especially of religious and civilization conflicts. The most representative reason to be mentioned is the civil war in Syria, followed by the Saudi-Iranian conflict and the Arab-Israeli conflict. Many cyber-attacks or acts of cyber terrorism were caused by the parties involved in the Syrian war. The Syrian army has used various methods of social engineering and malicious software to attack users and anti-government organizations in Syria and other countries.

In Iran, the most common attack was in 2010 on energy infrastructure. This attack was produced by the Stuxnet virus, which destroyed the centrifuges used in the process of enriching nuclear fuel. After that, another virus that was discovered by the Iranian authorities is the Flame virus, which attacked the computers of Iranian officials. This virus was designed to spy out the Middle East cyberspace by attacking operating systems that used Microsoft Windows (Sanger, 2012). Another major attack was in August 2012, when Saudi Arabia's largest Saudi oil company was attacked with the Shamoon virus, killing more than 30,000 computers. (Microsoft, 2018) Two weeks later, a similar attack took place on Ras Gas in Qatar, a giant in the gas market. At a time when security professionals recommend last generation identity management techniques such as facial recognition and biometric identification, only 80% of large Gulf businesses continued to

use usernames and passwords as the only means of connecting (Microsoft, 2018). Environments such as the gas, oil and utilities industries will still be at risk of being hit by cyber-attacks.

This year, the Middle East PwC study on the global information security situation shows that these security challenges are likely to grow only in the region, while sophisticated technology is continually expanding. Despite an annual increase in strategic initiatives to improve security among Saudi Arabian enterprises, it continues to be a hot target for cyber criminals, given the geographic, political and economic position of the region.

Figure 2: Types of cyber-attacks observed in the both regions (Source: Author's own processing based on EG-CERT Report and International Institute for Counter-Terrorism)

Middle East	North Africa
Web defacement	Mass Defacement
Spam	Web site defacement
Spoofing	Malware
Proxy Scan	DDOS
Denial of Service	Phishing
Distributed Denial of Service	SQL Injection Attack
	Session Hijacking and
Malicious Codes	Man-in-the-Middle Attacks
Virus	Credential Reuse
Bots	Cross-Site Scripting (XSS)
Data Theft and Data Manipulation	Others
Identity Theft	
Financial Frauds	
Social engineering Scams	

This makes it difficult for companies to identify when an attack occurre. Many are identified when third parties or customers report suspicious messages or requests for funds. But early detection and effective incident handling require a comprehensive and integrated security plan that takes into account all critical parts of an organization. It's just that all these things are not enough if the organizations personnel are not trained to cope with incidents, as attacks range from direct theft of data through hacking, spamming, phishing, DDoS attacks etc. Attackers are becoming more and more innovative and are using innovative types of attacks, which makes it easier to access systems. There is no limit of the negative impact that a cyber incident may have on an organization in today's digital age.

From loss of customer and employee data to financial losses caused by fraud or business interruptions, the list of risks is long. Each company or institution has a unique exposure to digital risk that is closely related to the nature of the organization and should, therefore, be identified and mitigated fully and carefully at all levels.

Trends in North Africa

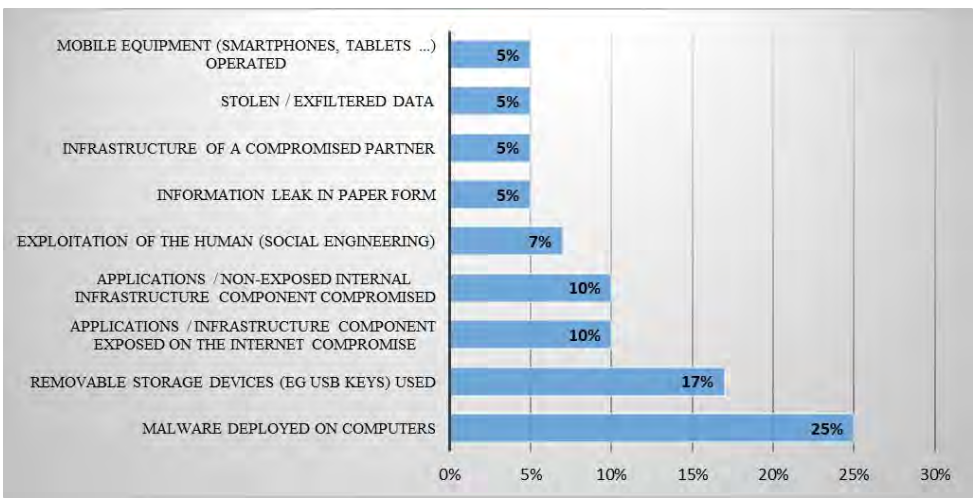
Algeria has made significant progress in the IT sector in the recent years. Following strong investments made over the last three years, the country has updated its legal framework and has introduced a number of new regulations to support the growth of the IT sector. Like other states in the region, the Algerian government has identified a number of cyber security issues in the sense that there is no well-grounded legislative framework that provides measures to counter cyber terrorism and that some of the population is considered vulnerable to possible threats. Like the European states, Algeria has improved its legislation on personal data protection and the creation of mechanisms to prevent online fraud and copyright infringement (Oxford Business Group).

With regards to Egypt, the main cyber threats faced it are threats of intrusion and sabotage of IT infrastructures, cyberterrorism, cyberwar, digital identity threats, and theft of private data. At the end of 2018, the Supreme Council of Cyber Security (ESCC) has launched the National Cyber Security Strategy. According to the strategy, a period of

four years, the government will implement six specific programs to guarantee the citizens' security on the Internet and of electronic payment systems. According to the Global Cyber Security Index, Egypt is Africa's leading cyber security and cyber-awareness campaigns among the population (Ecofin Agency, 2018).

Cyber-crime has become a concern for Moroccan IT companies as well as industry, service and communication. According to a study by PwC for IT companies, the results showed that more than 70% of respondents believe that their security systems do not meet all the standards of the global cybernetic system. Moroccan companies face a challenge caused by the digitization of almost all activities, but also by the fact that they do not have the technical ability to detect the actions of cybercriminals early on. (PwC, 2018)

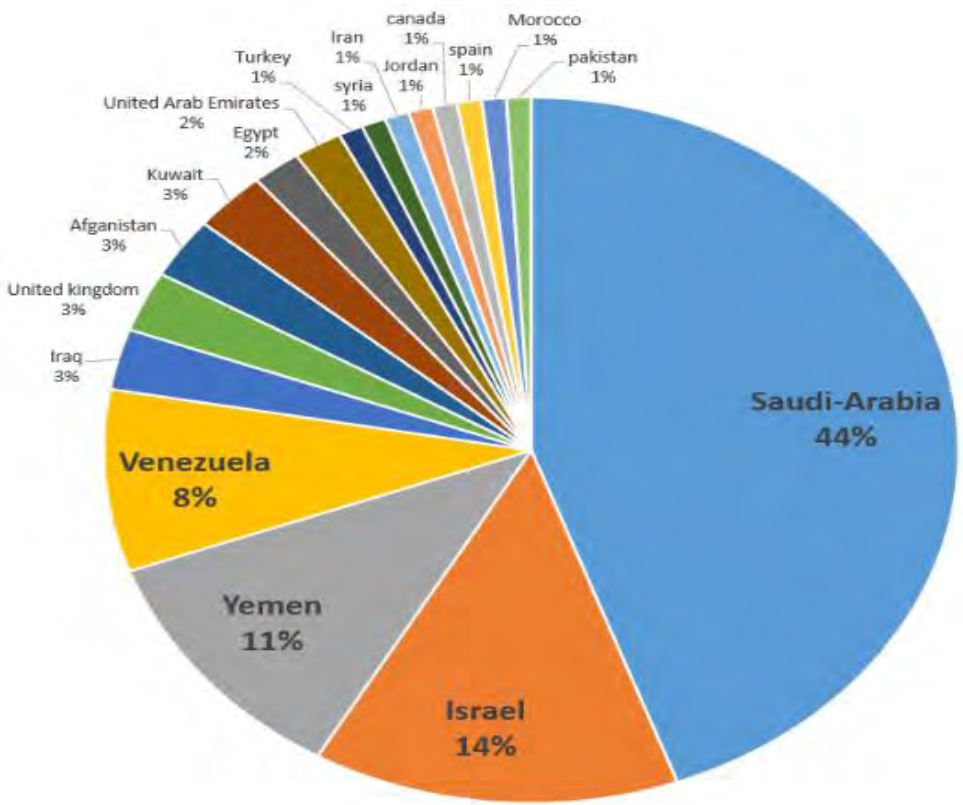
Figure 3: The nature of the incidents detected in Morocco (Source: Author's own processing based on PwC Global State of Information Security Survey 2018)



A threat that has been faced by Tunisia since the outbreak of street protests in 2011 is the impact of social networks on young people and their possible radicalisation. Through these networks, terrorists have been able to easily identify target groups and disseminate their

propaganda messages. In addition to the techniques underlying terrorist activities such as commissioning, communicating, training and executing attacks, these groups have increased their defence capabilities through websites. Among the most common online risks faced by citizens, institutions and companies are: compromising personal information through espionage, piracy and theft. In order to prevent cyber incidents and to inform the public of the risks they are facing on the Internet, the government has launched in September 2018 the e-portal "Tunisians against Cyberterrorism" (Centre for Applied Policy Research, 2018).

Figure 4: Cyber target distribution by country
(Source: Clear Sky Cybersecurity Report, 2015)



Major Cyber breaches in the Middle East and North Africa

The most active hacker groups are Iranian. Below we will detail the major attacks committed by these:

- Saipem in Italy was attacked with a Shamoon malware program and its servers were directed to Middle Eastern countries by Iranian groups. This program was previously used in an attack on 30,000 computers by the Saudi Aramco oil giant (Brewster, 2018). Iranian groups have been behind attacks on the Government and communications infrastructure, dozens of Internet sites belonging to Middle East, North Africa, Europe, and North American entities (Tweed, 2019).
- In February 2014, a group of hacked-ups attacked Sands in Las, through computers and mobile phones (Bloomberg, 2014). In 2015, a cyber spying campaign called the Thamar Tank was launched against Middle East University researchers, defence and security companies, journalists and human rights activists (Clear Sky Security, 2015).
- In 2017, the APT33 group entered the servers of an American airline, a Saudi Arabian airline, and a South Korean petrochemical company, where it stole commercial secrets (O'Leary et al., 2017). In 2018, the Oil Rig cyber spy group, which acts primarily in the Middle East, has carried out an APT attack and data theft against several states (Lee and Falcone, 2018).
- In May 2017, an attack against the HBO television station was made through a data theft scheme and it resulted with the loss of $ 6 million by the use of Bitcoin (United States Department of State, 2017). In 2018, the Leafminer group has attacked government organizations and companies across the Middle East using security grids, trying to access email addresses, servers, and sensitive information databases (Symantec, 2018).
- March 2018, a report from the UN showed that North Korean hackers have been trying to compromise the

email accounts of members of a UN commission that applies trade sanctions against North Korea. (Centre for Strategic & International Studies, 2019)

- April 2018 – Israeli cyber scientists have reported that Hamas has installed spyware in Fatah mobile phones that is a rival Palestinian faction. (Centre for Strategic & International Studies, 2019)
- November 2018 – The Chinese state's media said the country was the victim of multiple attacks by foreign hackers in 2018, including the theft of confidential emails, utility design plans, armed lists, and many other confidential information. (Centre for Strategic & International Studies, 2019)
- November 2018 – North Korean hackers have used various mauves to steal tens of millions of dollars from Asia and Africa. (Centre for Strategic & International Studies, 2019)
- December 2018 – North Korean hackers targeted the Chilean interbank network after an employee installed malware in a fake job interview. (Centre for Strategic & International Studies, 2019)
- December 2018 – Chinese hackers have compromised EU communications systems, retaining access to various diplomatic channels for many years. (Centre for Strategic & International Studies, 2019)
- December 2018 – North Korean hackers have stolen personal information from more than 1,000 North Koreans who live in South Korea. (Centre for Strategic & International Studies, 2019)
- December 2018 – The US, Australia, Canada, the United Kingdom and New Zealand have accused China of running cyber spying campaigns for nearly 12 years and are targeting the IP and business secrets of companies in nearly 12 countries. (Centre for Strategic & International Studies, 2019)

- December 2018 – US Navy officials have declared that Chinese hackers have repeatedly stolen information from the Navy contractors, including information and ship maintenance data and missile plans. (Centre for Strategic & International Studies, 2019)
- January 2019 – The United States Department of Justice has declared that an operation to disturb the media, aerospace, financial and critical infrastructure has come from North Korea. (Centre for Strategic & International Studies, 2019)
- January 2019 – A former American intelligence officer was found to work for the UAE to help the country learn more about diplomats, government officials, and their activists. (Centre for Strategic & International Studies, 2019)
- January 2019 – Security researchers have shown that Iran's hackers have been targeting the telecommunications and transport industries since 2014. Their purpose was to collect and supervise people in the Middle East, the US, Europe, and Australia. (Centre for Strategic & International Studies, 2019)
- January 2019 – The South Korean Ministry of National Defence declared that a group of unknown hackers compromised the information systems of the ministry's procurement office. (Centre for Strategic & International Studies, 2019)
- February 2019 – The airline Airbus said Chinese hackers, have stolen personal information to identify their European employees. (Centre for Strategic & International Studies, 2019)
- February 2019 – The Norwegian software firm Visma has declared that it was targeted by the Chinese Ministry of State Security hackers. They seem to have tried the commercial secrets of their business customers. (Centre for Strategic & International Studies, 2019)

Estimated trends of the next years

If the methods applied by traditional offenders in the physical world, such as extortion, armed robberies or drug distribution, have evolved over decades, cyber threats are subject to a rapid changing process, as cyber attackers use another type of attack every day.

Figure 5: Top 5 Global Risks in terms of impact
(Next 10 years, source: World Economic Forum Global Risk Perception Survey 2018-2019)

In figure 5 we can see what cybernetic trends are in the next 10 years. The year 2017 was one in which new types of attacks arose, affecting three quarters of world countries, such as Wannacry, NotPetya, Locky, GoldenEye and Jigsaw, which spread around the world in a few hours, some of them targeting to show the vulnerability of systems while others aimed to gain cash rewards. These threats have continued in 2018 with the same intensity, causing major IT infrastructure damage all over the world.

The Trends for the coming years require the businesses to improve their capabilities to protect business information, as hacking groups are always looking for a new way to mount stolen information and access to servers. An example of this is the $ 81 million that disappeared following a cyber-attack from a bank in Bangladesh in just a few hours. Governments around the world must prioritize collaboration and information sharing to develop new cyber security programs. Also it should be maintained the communication with telecommunication companies and service providers in order to build together means of preventing cybercrime.

Conclusion

The Middle East and North Africa are the home of many cyber-attacks occurring around the world, but at the same time they are also beneficiaries of these attacks. Some countries have poor legislation and have an outdated and vulnerable technology against threats they are facing each day. Among the countries with strong legislation and an annual budget that grows from year to year precisely to deal with threats and companies benefit from competitiveness. And the trends in the next years are based on state-private cooperation to prevent cyber-attacks.

References:

1. Agbugah, F., (February 18, 2015). *Moroccan Banks Are The Latest Victims Of Cyber Attacks.* [Online]. Available at http://venturesafrica.com/ moroccan-banks-are-the-latest-victims-of-cyber-attacks/ .

2. Elgin, B., Riley, M., (December 12, 2014). Now at the Sands Casino: An Iranian Hacker in Every Server," Bloomberg. [Online]. Available at https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas#p1

3. Brewster, T., (December 13, 2018). Warnings as Destructive 'Shamoon' Cyber Attacks Hit Middle East Energy Industry. Forbes. [Online]. Available at https://www.forbes.com/sites/thomasbrewster/2018/12/13/warnings-as-destructive-shamoon-cyber-attacks-hit-middle-east-energy-industry/#68e4e1713e0f.

4. Centre for Applied Policy Research (October 10, 2018). *Fighting Cyber Terrorism, improving Cyber Security in Tunisia*. [Online]. Available at https://www.cap-lmu.de/aktuell/events/2018/cyber-security-tunisia.php.

5. Centre for Strategic & International Studies, (2019). Significant Cyber Incidents from 2018 and 2019. [Online]. Available at https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

6. Check Point, (2018). *Check Point Cyber Attack Trends: Mid-Year Report 2018.* [Online]. Available at https://research.checkpoint.com/wp-content/uploads/2018/07/Cyber-Attack-Trends-2018-Mid-Year-Report.pdf.

7. Clear Sky Cybersecurity, (June 2015). Thamar Reservoir. An Iranian cyber-attack campaign against targets in the Middle East. [Online]. Available at https://www.clearskysec.com/wp-content/uploads/2015/06/Thamar-Reservoir-public1.pdf.

8. Ecofin Agency, (December 12, 2018). Egypt *launches its 2017-2020 national cybersecurity strategy*. [Online]. Available at https://www.ecofinagency.com/telecom/1212-39420-egypt-launches-its-2017-2020-national-cybersecurity-strategy.

9. Gjelten, T., (2013). *Cyberattacks, terrorism top US security threat report*, [Online]. Available at, http://www.npr.org/2013/03/12/174135800/cyber-attacks-terrorism-top-u-s-security-threat-report. Accessed 10 November 2014.

10. McFarlin, J., (2014). *ISIS cyber ops: Empty threat or reality?* [Online]. Available at http://www.securityweek.com/isis-cyber-ops-empty-threat-or-reality. Accessed 11 November 2014.

11. Lee, B., and Falcone, R., (July 25, 2018). OilRig Targets Technology Service Provider and Government Agency with QUADAGENT, Palo Alto, [Online]. Available at https://researchcenter.paloaltonetworks.com/2018/07/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/.

12. Oxford Business Group, *Algerian ICT expands on digitisation and cybersecurity*. [Online]. Available at https://oxfordbusinessgroup.com/overview/increased-competition-alongside-digitisation-and-cybersecurity-efforts-arrival-new-players-has.

13. Panda Security, (January 25, 2016). *27% of all recorded malware appeared in 2015.* [Online]. Available at https://www.pandasecurity.com/mediacenter/press-releases/all-recorded-malware-appeared-in-2015/.

14. PwC, (May 2018). *Global State of Information Security Survey 2018.* PricewaterhouseCoopers France and Francophone Countries of Africa, p. 14. [Online]. Available at https://pwcmaroc.pwc.fr/fr/publications-communique-de-presse/comment-entreprises-maroc-apprehendent-cybersecurite.html.

15. Sanger, D.E., (2012). Obama order sped up wave of cyberattacks against Iran , http://www.nytimes.com/2012/06/01/world/middleeast/obama -ordered - wave -of -cyberattacks -against -iran.html?page- wanted=all, Accessed at October 10, 2015.

16. Symantec, (July 25, 2018). Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions, [Online]. Available at https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east.

17. Tereshchenko, N. (2013). *US Foreign Policy Challenges: Cyber Terrorism & Critical Infrastructure* [Online]. Available at http://www.e-ir.info/2013/06/12/us-foreign-policy-challenges-of-non-state-actors-cyber-terrorism-against-critical-infrastructure/. Accessed, 11 November 2014.

18. Tweed, D., (January 11, 2019). Iran Hackers Could Be Behind Wave of Cyber Attacks on Infrastructure: FireEye. [Online]. Available at https://www.insurancejournal.com/news/international/2019/01/11/514571.htm.

19. U.S. Department of Justice, (November 21, 2017). Press Release, Acting Manhattan U.S. Attorney Announces Charges Against Iranian National For Conducting Cyber Attack And $6 Million Extortion Scheme Against HBO, [Online]. Available at https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-charges-against-iranian-national-conducting.

20. World Economic Forum, (2019). These are the biggest risks facing the Middle East and North Africa. [Online]. Available at https://www.weforum.org/agenda/2019/04/these-are-the-biggest-risks-facing-middle-east-and-north-africa/.

21. Ziffer, A., (February 19, 2019). *Cyber-attacks by foreign governments, malicious companies and enterprising hackers are on the rise. And the biggest problem is you.* [Online]. Available at https://www.abc.net.au/news/2019-02-20/cyber-crime-hits-consumers/10825970.

TEACHING APPROACHES FOR THE KEY ACTORS IN COUNTERING RADICALISATION AND BUILDING A RESILIENT SOCIETY

Ioana CHIȚĂ[*]
Irena CHIRU[*]

Abstract

In recent years, radicalisation has greatly evolved. Armed conflicts from failed states have boosted radicalisation inside the EU, and the rise of foreign terrorist fighters (FTF) is only an example. Thousands of the EU citizens have joined the war theatres of Syria and Iraq. As a result, radicalized returnees with combat skills and indoctrinated against European values pose a great threat to the security of EU. Furthermore, terrorist propaganda led to uncoordinated attacks of home-grown lone actor terrorists, difficult to detect before they strike. A response strategy to the above mentioned societal trends might be dealing with their root causes. Education and good quality training remain at the central core of building a resilient society against extremist ideologies and radicalisation, as well as of having first line practitioners that hold expertise.

Practitioners like intelligence officers, community police officers, prison and probation officers, law enforcement, youth and social workers, healthcare professionals and others, are valuable key actors in the prevention and combat of radicalization. Each one of them provides a part of the solution; there is no single actor that can prevent the phenomenon on its own. Therefore, it is important that they all know how to contribute. Training practitioners in the spirit of creating a multi-agency network where they can share both expertise and information is a key solution to efficiently combating radicalization. In addition to this, having a society resilient to radicalisation is part of the wider desideratum of promoting a security culture among civil society. Building a resilient society means transforming teaching institutions into "labs for democracy" and "training the teachers" because they are at the frontline when it comes to potentially identifying early signs of radicalisation, besides raising awareness through educational programs and public campaigns or round tables that address the topic.

Keywords: *radicalisation, training practitioners, building resilience*.

[*] PhD Student at "Mihai Viteazul" National Intelligence Academy, ioana.matei@animv.ro
[*] Professor at "Mihai Viteazul" National Intelligence Academy, irena.chiru@animv.ro

Introduction

In recent years, the terrorist phenomenon continues to pose a real threat at European level. In 2018, EU Member States reported a total of 129 terrorist attacks foiled, failed or successfully completed (TE-SAT, 2019). Islamist radicalization being one of the ideological engine which underlies the phenomenon. One of the causes for this is online propaganda. The INTERNET is currently the favourite environment for radical content due to obvious reasons: information is accessible, it facilitates real-time interaction with people from all around the world that have similar beliefs and on-line activities are anonymous.

In 2018, terrorist organizations and non-affiliated sympathizers diminished their use of mainstream platforms such as Facebook, Twitter and YouTube to disseminate radical content, increasing the use of start-up social media[1] (over 150 in number) (IOCTA, 2019) and of file sharing sites. Older propaganda materials are redistributed by new means. Some terrorist fundraising campaigns are also running on the Darknet (IOCTA, 2018).

Daesh's propaganda machine has encouraged lone actor terrorism. The destruction of the Caliphate did not remove the spreading causes of the jihadist terrorism on European territory due to repeated attempts by the organization to translate the idea of Caliphate into the on-line. The Daesh propaganda has shifted in the direction of encouraging European sympathizers to launch attacks against Western states in support of a "virtual Islamic state".

Daesh's non-affiliated sympathizers clotted into the home-grown terrorist trend which targets symbols of authority (Carcassonne, March 2018[2]), or indiscriminate attacks of civilians (Paris, May 2018[3]). Jihadist attacks are mainly committed by radical terrorists in their own country of residence, without traveling to a war theatre to join a terrorist

[1] Examples include Threema, Signal or Telegram.
[2] On 23 March 2018 a Moroccan male wounded and shot four policemen and two civilians, injuring several others. He also held the customers of a supermarket in Trebes hostage.
[3] On12 May 2018 a French citizen killed one person and injured several more in Paris, before being shot dead by the police.

organization. These actors are very diverse, being born or living largely in the EU. Most of them are known to the police, but not for terrorist activities, and often do not have direct links with Daesh or any other jihadist organization (IOCTA, 2019).

The *home-grown* terrorist trend emerged in a security context already characterized by vulnerabilities such as the migratory pressure and the associated risks, namely the infiltration of Daesh combatants and *returnees* into the migratory flows. European citizens who joined the organization into the jihadist theatre (*foreign terrorist fighters/ FTF*) have the possibility now to return to the EU member states taking advantage of their citizenship. FTFs pose major risks for the security status of the entire "common" space due to their military training and combat capabilities, high level of indoctrination and good counter-intelligence skills, which facilitates them to pass unnoticed by the national intelligence services.

The degradation of Daesh's organizational structures may reduce the attractiveness of the group, but it will not affect the threat posed by jihadism because individuals and sympathizers disillusioned with the Islamic State – including those living in EU Member States – may refocus on other terrorist groups. Al-Qaeda maintains itself as a strong and active key actor who seeks to fill in the power gap present in the jihadist arena and continues to encourage terrorist attacks in the EU and beyond. The terrorist activities guided or inspired by al-Qaeda or other jihadist organizations remain a realistic possibility for the EU's close future (TE-SAT, 2019).

The radicalization process

To better understand terrorism, first of all, it is necessary to analyse the underlying phenomenon, which is (self) radicalization. A wide range of formulas have been proposed to define (self) radicalization, all of which have as a common element the fact that **some individuals adopt ideologies or beliefs on behalf of which they commit terrorist acts**. These individuals give up a common life to "make justice" for the community or for themselves and may be Westerners vulnerable to jihadist propaganda, migrants, refugees, asylum seekers, prisoners, probationers or members of the Muslim

diaspora who, due to social polarization and failure to adapt in the European host countries, can turn to radical views.

Current research has shown that radicalisation is caused by multiple causes. Gøtzsche-Astrup (2018) analysed the literature on the psychological mechanisms of radicalisation and discovered that social motivational processes are essentially driven by primitive mechanisms of aggression (Gøtzsche-Astrup, 2018). Also, negative life experiences can act as "triggers" of radicalisation because the individual starts raising fundamental existential questions. This can be exploited by subcultures offering alternatives and manufactured answers.

The dynamics of small groups represents a key factor in converting radical belief into action by accentuating polarization. Strong emotions, such as anger and contempt, are important motivational factors. Another motivational factor is the "dynamics of self-identity and of social identity" which, through a fractionalization process, contributes to raising individual's confidence in the social identity of the specific group.

The sociologist Kevin McDonald argues that radicalisation is a social process that involves exchanges, connections and shared emotions. This implies that someone's ability to feel certain things makes it possible for that person to think those aspects. In this sensory process, the social media and jihadist culture play an important role.

Some researchers have studied acculturation and its potential role in the radicalisation process: individuals who do not have a good relationship with their parents and feel rejected by the society, embrace another culture that gives them a sense of belonging, which instead can lead to radicalization.

Campelo *et al.* (2018) mention a multitude of factors that make the individual more vulnerable to radicalization: individual factors such as psychological vulnerabilities (depression, addictive behaviour, abandonment at an early age, trauma, the death of someone close etc.), micro-environmental factors (such as the friendship with a radicalized person, family dysfunctions), or macro-environmental factors like social polarization, religious ideology or the geopolitical context. In the same regard are the conclusions of the Radicalisation Awareness Network (RAN, 2016) that indicate the socio-psychological, social, political,

ideological and/or religious factors, cultural and identity factors, trauma and other trigger events, group dynamics and social-media role as being responsible for radicalisation.

Understanding radicalisation implies multi-causal explanations: there is no standard profile of radicalized individuals and the pathways to radicalisation are diverse. Radicalisation is a complex social issue that research has attempted to explain through a mix of factors originating from distinct sciences: sociology, psychology, psychiatry etc. Therefore, an effective response to this phenomenon implies inter-disciplinary cooperation and collaboration among practitioners from all the above mentioned areas.

This multi-dimensional challenge requires multifaceted responses involving all relevant policies and all relevant actors at local, regional, national, European and international level (HLCEG-R, 2018). Multi-agency working formats can provide adequate support for vulnerable individuals from an early stage.

Education as a response to the needs of practitioners in the field of prevention and combat of radicalization

For a long time it has been thought that preserving the national security status is under the exclusive privilege of intelligence and security field actors, whose institutional culture is defined by exclusivity and secrecy. However, the combat and prevention of radicalisation, as we mentioned earlier, requires multi-disciplinary practitioners acting in order to achieve a common goal.

Cooperation in an integrated manner of the empowered institutional actors is important for dealing with radicalisation cases efficiently. Practitioners need to learn to adapt to a new paradigm where more and diverse actors collaborate and share the responsibility of an area that is no longer under the exclusivity of one institution.

Professionals from different domains need to cooperate for an unique purpose in an integrated manner and contribute through skills, knowledge and support to prevent and counter the radicalisation process. Responsibility lies with practitioners in areas such as intelligence and national security, law enforcement agencies, police, the

penitentiary and probation systems, health and social care, child protection, psychology, psychiatry and education.

The first step for readjusting the institutional actors with responsibilities in intelligence and national security is learning to do so. Learning is essential for maintaining a spirit of professional adaptability in such a dynamic field like anti- and counter-terrorism.

In this new context, there is a need to develop training programs that teach a new mechanism of collaboration between the actors involved in the combat of radicalisation. These programs of learning need to approach within its curriculum the phenomenon, the role of each actor involved and the cooperation mechanism mentioned. The aim of the learning program is to form new competences for a unitary approach within a generally accepted framework, bringing together all institutional actors in an action plan and a homogeneous structure.

This initiative is intended to lay the foundation of a multi-agency cooperation mechanism already in place in other countries. An example of this type is the Respect.lu in Luxembourg, which has been operating since 2017 and it comprises 4 psychologists, a communications manager and a director. The centre provides prevention and awareness-raising services, individual therapeutic support, therapies for families and friends, social therapy and reintegration, training and workshops. The multi-agency network brings together representatives from various institutions and associations to create partnerships within the health, education, social, judicial and media sectors. Another example is Croatia where multi-agency structures were created ad-hoc, based on protocols explaining in detail the way authorities cooperate in the event of certain risks being materialized. United Kingdom also implemented such a multi-agency approach in dealing with prison radicalisation cases. The mechanism operates under a legislative framework called MAPPA – Multi Agency Public Protection Agreement – which brings together several authorities and services that evaluate the release conditions for each radicalized detainee.

The learning programme we propose in this paper consists of a workshop dedicated to practitioners at national level on how to cooperate in order to prevent and combat Islamist radicalisation. The

workshop includes two distinct sections: a theoretical module and a practical one (according to the structure presented below).

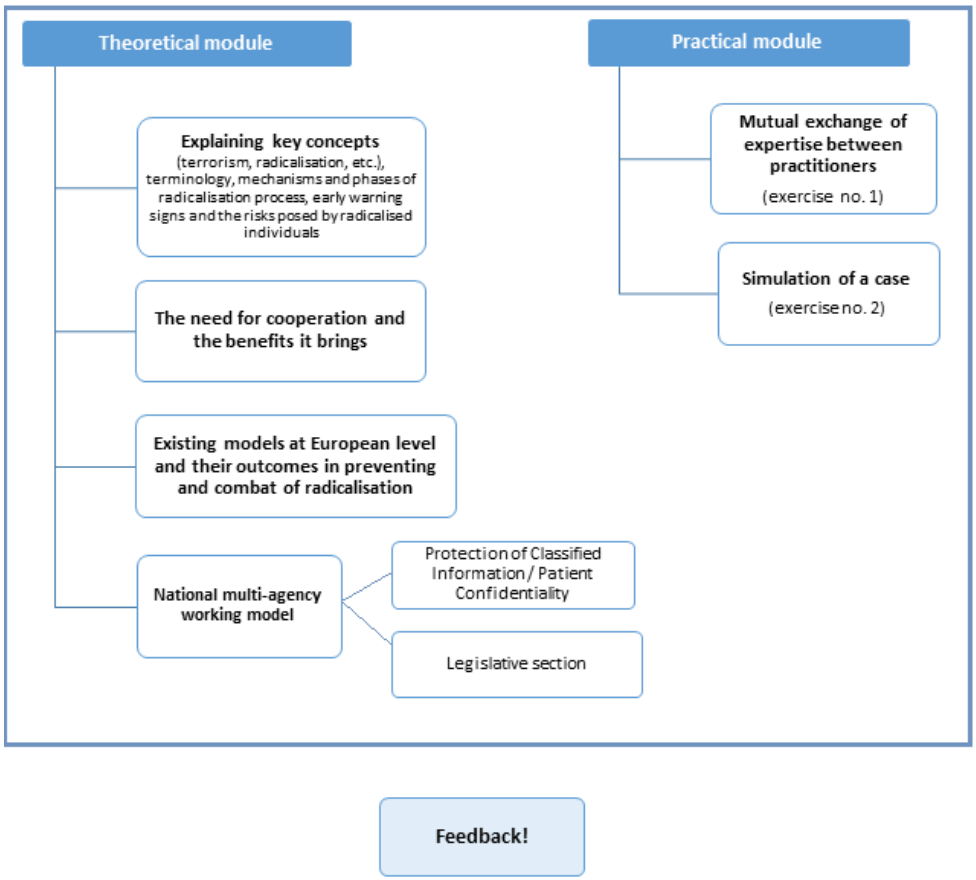


Figure 1: The structure of the learning programme proposed

The theoretical part of the workshop is imposed by the need to know of the participants who are not only practitioners in intelligence and national security, but also social workers, psychologists, psychiatrists or penitentiary staff etc., who by the nature of their professional experience are not necessarily familiarized with the concept of radicalisation. It is, therefore, essential that this workshop includes **a theoretical part focused on explaining radicalisation and**

other basic concepts like terrorism, Islamist fundamentalism, *foreign terrorist fighter, lone actor* etc., the specific mechanisms and stages of radicalisation, characteristics, risks involved and early warning signs.

Understanding terrorism and its underlying mechanisms facilitates a better comprehension of the way experts can use their own knowledge and professional background in the benefit of prevention and combat radicalisation. Understanding the concepts, terminology and the early warning signs of radicalisation can contribute as well to having a common language for practitioners coming from different domains with distinct visions, which later facilitates communication and collaboration.

It is necessary that the workshop stresses the need for practitioners to have a transversal collaboration and highlights the benefits of the multi-agency approach. The workshop needs to include a presentation of the existing models of multi-agency working (MAW) formats that tackle radicalisation and the good practices available at European level (as are the cases of Germany, Belgium, France, Finland, Luxembourg, Lithuania and Croatia). This will also include the results obtained by the earlier mentioned states in preventing/combating radicalization.

In addition to the above, the theoretical module of the workshop will present a national multi-agency working model which includes intelligence services and law enforcement agencies, on the one hand, and other practitioners, on the other hand, working together in order to prevent and combat radicalisation.

The model will take into consideration the challenges posed by the regulations regarding classified information / patient confidentiality in the case of partners from the health sector. Specifically, it will explain how an intelligence officer can collaborate with a healthcare service worker without violating the rules of classified information or patient confidentiality. This involves explaining the distinction between classified and sensitive information that could be shared with caution, the principle of reciprocity, the principle of prioritizing the national interest etc.

Furthermore, a legislative section on the legal provisions and mechanisms that can support cooperation through partnerships and establishing a coordinating institutional actor will be necessary.

If professionals with different backgrounds (police officers, psychologists, teachers etc.) co-operate, difficulties may arise from the difference in professional vision (scientific knowledge, experience, values, terminology etc.), which makes communication and ultimately achieving the common goal even more difficult.

In this respect, the applicative side of the workshop involves an interactive area in which practitioners exchange expertise for raising awareness on the difficulties, experiences and challenges faced by each other. Sharing of the experiences and difficulties faced by intelligence officers will take into account the need to anonymize the information and the cases presented.

An important aspect is to invest in mutual trust and understanding before continuing to develop a cooperative structure. Reciprocal trust is a significant component for any multi-agency approach. This can be achieved through exercises based on expertise exchange. The goal is to determine the actors involved to become conscious about each other's role in the process of preventing and combating of radicalization. Clarifying the role of each professional sets the right expectations and the tasks of each actor to achieve the final result, which are essential conditions for success.

The second part of the workshop is a simulation exercise of a real situation in which practitioners will have to work together in order to prevent and combat radicalization as part of a multi-agency mechanism. The simulated situation is an anonymous case that includes most of the key issues that practitioners can encounter: lack of a common terminology, absence of mutual trust, shortage of knowledge of the role and skills of the other etc. At the end, participants will provide feedback on the exercise, on ways for improving cooperation in order to optimize results and their final conclusions.

The applicative side of the workshop is designed to demonstrate the reliability of the mechanism and to test the willingness of practitioners to engage in this line of work. Its main role is to raise awareness on the necessity of cooperation in one of the main areas of

action of the Romanian Intelligence Service, which is the Prevention and the Combating of Terrorism, and will subsequently be the basis of creating a MAW mechanism for preventing and combating radicalization at national level. MAW formats are not the only available responses to radicalization but they provide a comprehensive framework in which cases of *lone actors*, FTF/*returnees*, refugees/ asylum seekers are addressed through the involvement of all competent institutional actors, taking into account possible issues such as trauma and/or mental disorders.

The Romanian Intelligence Service is the national authority in the field of preventing and combat of terrorism and, implicitly, Islamist radicalization. The Service has the required institutional resources to run such a workshop via "Mihai Viteazul" National Intelligence Academy that provides ongoing training programs for the personnel of the Service in various areas and professional fields.

The role of education in building a society resilient to radicalization

The society and, implicitly, the citizen is the main beneficiary of the activity of institutions responsible with the prevention and combat of terrorism. In the current state of security, society can no longer be a passive beneficiary and can become an active contributor to maintaining the national security status. This can be achieved through adequate education, by raising awareness on the phenomenon of radicalisation and self-radicalisation.

In preventing and combating radicalisation, resilience is often considered a precautionary measure based on the assumption that young people can be educated to withstand the attractiveness of recruits and agents of radicalisation. Resilience is defined as the ability to cope, learn and even evolve in the face of change, challenge and adversity (Cahill, 2008). So, in terms of resilience to radicalization, this implies the ability to rebalance after a deception, a personal crisis, perceived/ real injustice or dissatisfaction. In this respect, resilience involves questioning the "us vs. them" narratives characteristic to the radical propaganda discourse.

Resilience is a normal human adaptation process present both in young people originating from high-risk environments (poverty, parental conflict etc.), as well as in the cases of those raised in healthy environments.

Studies demonstrate that protective factors of resilience produce positive results for a percentage ranging from 50% to 80% of the children growing in high risk environments. The obvious conclusion is that efforts focusing on **strengthening personal skills and protective factors** that promote youth resilience in the family, community and schools (Benard, 2004) are more effective than those aimed at removing the risk factors that reduce resilience.

Education is the cornerstone in effectively preventing radicalisation by increasing resilience to radical propaganda and recruitment. Although, schools cannot influence all protective factors that increase resilience to radicalization, a good school experience can contribute solidly to this (Bonnell, 2011).

There are many reasons why schools play such an important role in the prevention and combat of radicalism. In the first place, it could be noticed that the age of those who joined the terrorist organizations in Syria and Iraq has fallen to 13-15 years (Van Ginkel, 2016), with young teenagers being a vulnerable group in the face of the phenomenon. Schools can provide a safe environment in which delicate issues such as social identity, immigration, social and international conflicts, discrimination, social marginalization can be addressed openly. In addition to these, schools can provide alternative narratives to the hate speech available in social media and can contribute to the development of critical thinking skills, which are essential in countering the effects of jihadist propaganda.

Teachers and educators play a crucial role in promoting social inclusion, common democratic values and managing controversial issues through open discussions in classrooms (HLCEG-R, 2018). Teachers are in the first line when it comes to observing early warning signs of radicalisation or unusual behavioural patterns in students. It is, therefore, important for teachers to be aware of their role, to be well trained to understand the phenomenon and how to contribute to an efficient mechanism of prevention and combat of radicalisation.

To begin with, this training needs to provide teachers with the necessary knowledge about the key concepts surrounding terrorism and radicalisation. Although we have all heard of radicalism, religious extremism and other similar concepts, in fact few people are aware of the phenomenon, its mechanisms, stages and early warning signs. A teacher is no exception to this despite the pressure parents and society in general put on teachers and educators to effectively manage all issues related to youths.

Practitioners (including teachers) involved in the prevention and combat of radicalisation need to have solid knowledge of the phenomenon to counteract the disinformation produced by jihadist propaganda, to question inaccurate assertions and to help young people develop constructive arguments and healthy lines of thought. Teachers need to be able, for example, to counter stereotypes or wrong assumptions about a particular religion or, if this is not feasible, to know how to access the necessary information.

Training the teachers to do so should take into consideration teachers' need of knowledge in terms of radicalisation, particularly the way it affects young people, main causes, the vulnerable categories of youth, the mechanisms and the stages of the process, risks posed by radicalized individuals and early warning signs.

Once teachers know these aspects, it is important that they become conscious about the role they can play in promoting a democratic discourse and in increasing the resilience of young people to radicalisation through effective teaching methods. Most of the key features of teaching methods that aim to increase resilience to radicalization are in fact general principles of good teaching: providing a "safe" space in classrooms where young people can express openly their opinion on sensitive issues in society, developing critical thinking skills, positive interactions in the classroom and a spirit of cooperation.

In order to prevent and combat radicalisation, schools can have a positive impact through classrooms that provide a safe space, meaning an area where participants feel safe to talk about controversial issues and express their views comfortably, regardless of the reactions they may cause. Facilitating a safe space for positive interactions and communication (for example, by using basic rules for dialogue, through the teacher's ability to resolve conflicts and by paying attention to the

needs of individuals) is an essential feature of any pedagogical method aimed at increasing resilience to radicalization. The teacher should be able to create such an environment that facilitates discussion on sensitive issues without experiencing negative emotions (frustration, anger, annoyance etc.).

A safe space for discussions provides the opportunity to mitigate the factors favouring radicalism as it offers the chance to explore grievances, feelings of injustice and real/perceived humiliating experiences, to express personal opinions (without which young people may feel frustrated and become attracted by terrorist groups exploiting their views) and to address the knowledge gaps that are used throughout the terrorist recruiting process.

Discussions must follow certain rules for a respect-based environment. A clear definition from the beginning of what positive and negative behaviours mean, gives equal rights and responsibilities to the discussion participants. Also, conversations must be inclusive, open and non-conflictual because not all participants have the confidence to share their opinion. The teacher must be able to respond effectively to emotionally intense conflicts. Sensitive and profoundly offensive statements must be dealt with through effective responses that maintain the safety of space and do not contradict their content, as it can enhance extremist attitudes and views.

Paradoxically, preconceived ideas must be respected by allowing young people to express their thoughts and feelings in their own way, even in cases where teachers do not agree with the opinions or the language used. These preconceptions may reflect extremist thinking, but rather than be ignored, teachers should allow views to be expressed and treated. The opposite situation makes vulnerable young people feel judged and less likely to engage constructively in activities to increase resilience to radicalization.

A relevant skill for all young people but particularly valuable for vulnerable people who may be targeted, exposed to or attracted by extremist propaganda is the analytical approach that allows youths to critically analyse propaganda and other messages they may encounter in the media (online, newspapers, television etc.). In classrooms, critical thinking should be encouraged. Critical thinking skills imply the ability to ask questions and not receive information and ideas from others

passively, to review a balanced range of evidence to analyse a situation, hypothesis, opinion or message, to realize that there are different perspectives from one's own and remain open to the integration of new points of view in personal thinking. Critical thinking competencies – essential to interrogating and challenging extremist ideologies – can be successfully developed through teaching methods that support intellectual research by young people themselves. To develop a mind open to "critical thinking", young people need to be actively encouraged to become aware of their own opinions and experiences, empathize and understand the reasons behind other people's vision.

Last but not least, a safe space for communication involves positive interaction within the group. By this we understand the ability to listen to others without provoking, to work collaboratively to achieve a common goal, to negotiate with others and to have patience in working with other persons. Teachers are the actors responsible for shaping such skills in young people.

Although the above-mentioned aspects are partly general features of good teaching, it is necessary to synthesize them in training for teachers and educators specialized on the responses to radicalisation through education. The training will be included in a two step approach consisting of two cascading workshops – the first one is the one dedicated to practitioners from different fields, including teachers, which will provide them the necessary knowledge on radicalization, while the second workshop is solely dedicated to teachers so that they can develop and practice the teaching methods that could ultimately lead to increasing resilience in schools through apropiate teaching methods.

Creating society resilient to radicalization through education is a reliable partner for preventing the phenomenon. Schools are the best places to increase youth resilience to extremist ideologies and to promote democratic values. To achieve this, we need to have well-trained teachers, better equipped schools, time and resources.

Conclusions

Education is the long-term response to many of society's issues, including radicalisation. Educating practitioners active in the field of

prevention and combating of terrorism must be constant and synchronized with the evolution of the terrorist phenomenon and the latest research in the field. Officers from areas such as intelligence and national security, police, prison and probation systems, doctors, social workers, child care assistants, psychologists, psychiatrists and teachers need to be aware that addressing such a complex issue like radicalisation is no longer under the responsibility of a single institution. Addressing Islamist radicalisation from a multi-agency working format makes it more effective.

The preventive approach also aims at educating teachers who, through enforcing good pedagogical practices, can contribute to increasing resilience to radicalization of young people. In addition to the fact that schools can act as incubators of radicalization and teachers are part of the first line of practitioners who can detect early warning signs of the phenomenon, a safe space in classrooms where delicate subjects can be approached without restrictions mitigates the factors leading to radicalization. Creating such an environment is the responsibility of the teacher who becomes one of the key actors in preventing and fighting the phenomenon.

The Romanian Intelligence Service – as a national authority in the field of prevention and combat of terrorism – has the potential to develop customized trainings for educating and raising awareness to the key actors in preventing and combating of radicalization. This can be achieved through "Mihai Viteazul" National Intelligence Academy that provides ongoing training programs for the employees of the Service and members of civil society, covering diverse professional areas and fields.

References:

1. Benard, B. (2004). *Resiliency: What we have learned.* San Francisco: WestEd.

2. Bonnell, J. C. (2011). *Teaching approaches that help to build resilience to extremism.* Retrieved from https://assets.publishing.service.gov.uk/

government/uploads/system/uploads/attachment_data/file/197224/DFE-RB119.pdf.

3. Cahill, H. (2008). *Building resilience in children and young people: A Literature Review for the Department of Education and Early Childhood Development (DEECD).* Melbourne Graduate School of Education & Youth Research Centre.

4. Campelo, N. O. (2018). Who are the European youths willing to engage in radicalisation? A multidisciplinary review of their psychological and social profiles. *European psychiatry*, 1-14.

5. CoE, R. (2016). *The root causes of violent extremism. RAN Issue Paper*. Retrieved from Radicalisation Awareness Network, Centre of Excellence: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network.

6. Event_Radicalisation. (2018). *University of Sydney*. Retrieved from https://sydney.edu.au/news-opinion/sydney-ideas/2018/radicalisation.html.

7. Gøtzsche-Astrup, O. (2018). The time for causal designs: Review and evaluation of empirical support for mechanisms of political radicalisation. *Aggression and Violent Behavior*, 90-99.

8. HLCEG-R. (2018). *High Level Commission Expert Group on Radiclisation.* Luxembourg: European Comission. Retrieved from https:// ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/ european-agenda-security/20180613_final-report-radicalisation.pdf.

9. Hogg, M. A. (2014). From uncertainty to extremism: Social categorization and identity processes. *Current Directions in Psychological Science*, 338-342.

10. IOCTA. (2018). *Internet Organized Crime Threat Assessment.* Europol.

11. McDonald, K. (2018). *Radicalization.* Polity Press.

12. TE-SAT, E. (2018). *EU Terrorism Situation and Trend Report .* Europol.

13. Van Ginkel, B. &. (2016). *The Foreign Fighters Phenomenon in the European Union. Profiles, Threats & Policies.* Hague: The International Centre for Counter-Terrorism.

INTELLIGENCE, SECURITY AND INTERDISCIPLINARITY

THREATENING LETTERS: MENTAL CONFUSION AND HATE AS MOST COMMON PREDICTORS OF ARREST FOR VIOLENT BEHAVIOUR

Margaret DIEKHUIS-KUIPER*

Motto: *You are going to die soon. If I find you I'll kill you.*
You are going to die just like Pim Fortuyn. One of these days you're going to be shot to pieces so better watch your step. All the Muslims are going to kill you, you won't be safe in the streets, and this is a hint. My nigga/Muslim friends are going to kill you in New York City. I'll kill you if I see you!! Who can I hire to shoot Wilders in the head?
If I catch you I'm going to smash your face in.

Example of internet threatening letters

Abstract

This study focused on digital and handwritten threats against individuals in what are known as the national security domain. Being threatened may stir up feelings of fear or unrest. Making threats towards people in the public domain can influence the public debate and may even jeopardize the democratic legal order when a fear of (repeated) threat stands in the way of open and frank discussion. Threats, and the subsequent assessment and decision-making process, are time-consuming and difficult, without other available documents. The main question was: which characteristics can be linked to criminal acts? Insights were gained from threat studies and from forensic linguistics to better understand the motives of those writing threatening letters. Bivariate- and logistic regression analysis were used for assessing characteristics in 450 letters. Mental confusion, which was operationalized in the theoretical framework as incoherent use of language, was linked to repeated threats. Mental confusion and hate increased the likelihood of being arrested for violence behaviour.

Keywords: *Public figures, violent behaviour, communicated threats, threat assessment, offender characteristics, forensic linguistics.*

* Forensic Psychologist, PhD, Ministry of the Interior and Kingdom Relations, email: Margaret.kuiper@minbzk.nl.

Introduction

The assessment of threats in relation to future (criminal) behaviour is a question that occupies the National Police, the Public Prosecution Service (OM) and also, for example, the intelligence and security services. What are the presumed intentions of those that write threatening letters and which words indicate an elevated risk that the threatener will put action to words? The internet invites us to communicate digitally, and in addition to handwritten threatening letters threateners also appear to choose this method (De Groot, 2010). Threats can cause feelings of fear and unrest in those that have been threatened and those around them. Threatened persons – and others – can feel intimidated, or experience feeling socially restricted in their thoughts, actions, and movements (Bovenkerk, 2005). When threats are directed against public figures, this can influence the public debate and even constitute a threat to our democratic legal order, and the fear of (repeated) threats can stand in the way of open and frank discussion (Bovenkerk, 2005). The focus of this study was on threatening letters and non-criminal threatening letters directed at public figures whose security and unhampered performance of duties are of national importance, for example politicians and royalty. The aim of the study was two-fold: on the one hand expand available knowledge regarding the characteristics of threatening letters, which could assist in interpreting the intentions of the writers of such letters, and on the other establish which of these characteristics are most related to the chances that a person will be arrested on suspicion of violence.[1] In this study, threatening letters was taken to mean: letters and emails in which public figures receive (in)direct death threats, or are wished dead (Meloy, 2000). The threatening letter can also state conditional threats (Bovenkerk, 2005; Meloy, 2000, 2001), such as: "*Ransom before 11 September 9am or else the prime minister dies.*" This study differentiates between criminal and non-criminal threatening letters. Non-criminal threatening letters are: letters and emails directed at

[1] This included assault and/or attempted manslaughter. Other criminal offences considered relevant in terms of acts of violence, are possession of arms and destruction of property.

public figures which at first glance do not seem to pose a threat. Their contents can be perceived as alarming or intimidating by those that receive them, for example because they contain a cry for help, incoherent use of language, threatened suicide, or a search for intimacy. In addition there were two relevant subgroups. The first subgroup concerned individuals that wrote only one letter. This group was compared to individuals that wrote letters repeatedly. In this study repeated letters are taken to mean: a second and possibly further letters written by one and the same individual. The second subgroup concerned individuals that were either arrested or not arrested on suspicion of a criminal offence after having written a first letter. Criminal offence in this study included assault and/or manslaughter, possession of arms, and destruction of property.

The idea behind this study was that behavioural experts or other assessors have to base their assessment on limited information, for example a letter. Such letters may contain valuable clues regarding the intentions and/or psychopathology of the writer, which is why it is relevant to analyse such missives (Dietz et al., 1991; Fein & Vossekuil, 1999; Meloy et al., 2004). The information provided by this process can also serve to provide greater security for the victim. The more accurate the prediction, the more thoroughly the police can provide coordinated security measures to protect the threatened person. In the assessment of a writer's intentions, the assessors generally rely on their experience, knowledge, and intuition. Although this approach is useful, this frequent method also constitutes a risk, because it is more susceptible to bias and false heuristics. Assigning greater importance to certain letters, or ignoring them, could result in bad decisions (Canter, 2000).

There has not been a great deal of qualitative scientific research, either nationally or internationally, into the phenomenon of threatening letters directed at public figures. In 2006 Smith studied threatening letters on the basis of an empirical analysis of the risks they constituted in the public and private domain. Smith focused on public and non-public figures, and for that reason that study is less comparable to the present one, which limited its focus to public figures whose security and unhampered functioning are of national importance. In 2014, James et.al. developed the CTAP-25, which is a generic measuring instrument

based on problematic letters in the public and private sector. CTAP-25 provides a triage score that is based on risk factors related to inappropriate communication or personal problems in, for example, a professional setting. Similar to the study by Smith (2009), CTAP-25 focused on problematic communications directed at public and non-public figures, and it is a generic risk management instrument for mapping problematic behaviour. In this study the focus was on the question whether the writer would act upon his threat and which words might be possible indicators of this. The focus, then, is on estimating the type of threat.

There are different types of threatening letters, in relation to which the main question is whether they provide enough elements to attribute meaning to the nature and form of the threat (Voerman, Brandt & Bullens 2014). This is a greater problem for digital and handwritten letters than for verbal/oral threats, as there is no direct social interaction between sender and receiver. In the present study information was collected from letters on the basis of a protocol and converted into quantitative data to be analysed. This means that the letter itself, rather than the contents of the (police) file, is used to assess whether the contents of the letter could provide information on background characteristics of the letter writer and their language use, and how this is related to later actions. Consequently the study had both an exploratory and a testing character. Firstly, characteristics or variables that are considered relevant to the assessment framework for the interpretation of letters or data were selected on the basis of the literature. The criteria were: which characteristics mentioned in descriptive studies of threatening letters can be related to future criminal behaviour? And which of these characteristics can be operationalised so that they can be used in a quantitative study? To assess this Cohen's kappa statistic was used (more on this under methodology).

This article will first look at the data set and what does the data set consist of? The development of the theoretical assessment framework – which methods and techniques were used to analyse letters? The section three discussed under methodology. The results are presented in section 4, illustrated by tables. Section five presents the conclusion and

discussion, and the article concludes with a series of recommendations in section six.

Data

Between 2012 and 2015 a total of 450 (digital and handwritten) threatening letters directed at persons in the public domain were collected for the purpose of this study. The letters concerned the period from 1999 – 2015. More specifically, 40% of the letters is from the period between February 1999 and January 2013 while the other 60% covers the period from January 2013 to February 2015. Part of the letter collection came from the Ministry of General Affairs, and part from the National Police. Some of the letters turned out to be doubles, because they existed in both a digital and physical format. After removing 172 doubles, a total of 278 letters remained. These letters were written by a total of 150 individuals.[2] Of these, 109 persons (73%) wrote only one letter and 41 individuals (27%) wrote more than one letter. These 41 repeated writers wrote 169 letters, an average of around four letters per person. Repeated letters were identified by equating the signature and/or handwriting in different letters. Remarkably, a large percentage (66%) of the 278 letters were signed with a first and/or last name, and sometimes also with an address (19%). In a number of cases a letter was signed anonymously, or with an alias or false name (15%). Although the letters were signed, of only 53 letter writers (35%) it was possible to ascertain in police systems (Blue View) whether the individual had been arrested on suspicion of a criminal offence, such as a violent act, after their first letter.[3] Of these 53 persons both their name and address were known, which was a decisive factor in whether someone could be traced in police systems and identified as a suspect.[4] The time between the first

[2] The identities of the individuals in this group were established on the basis of address, signature, micro features and page lay-out characteristics such as use of uppercase and lowercase, numbers, date of the letter, form of the letter.

[3] Here, violent act is taken to mean assault and/or attempted manslaughter. Other criminal offences considered relevant in terms of acts of violence are possession of arms and destruction of property.

[4] Generally speaking, first name, last name and date of birth are sufficient information to find someone.

letter and the last incident[5] which resulted in the suspect's arrest, was calculated to be almost 27 months on average. This high average was the result of the fact that for some letters there was a very long time – several years – between threat and arrest of the suspect. The median turned out to be 18 months.

Methodology

In order to be able to assess the intentions of writers of threatening letters with greater accuracy, an assessment framework (theory) and a protocol (questionnaire) were used to assess a collection of 278 letters for certain letter characteristics (Table 1).

Table 1: Overview of variables tested for occurrence in letters[6]

Background characterstics	*Presence (+) / absence (-)*	*Background characteristics*	*Presence (+) / absence (-)*	*Linguistic features*	*Presence (+) / absence (-)*
Cognitive distortions	+	Modi operandi (weapons)	+	Self-reference ('I')	+
Confusion	+	Fixation	+	Conjunctions	+
Incoherent language	+	Anger	+		
Negative coping	+	Hatred-revulsion	+	*Details*	
Burdoned frame of mind	+	Revenge	+	Micro features and page lay-out	+
Lack of remorse	+	Powerlessness	+		
Cause fear	+				

[5] Almost all letter writers featured more than once in Blue View; only the date of the last incident was used.

[6] Of the eighteen characteristics in Table 1, eventually only fourteen were used for the analysis; four were eliminated because the kappa was either insignificant or indeterminable.

Prosocial engagement	-
Positive coping	-

Some background elements, such as whether the writer suffers from depression or alcoholism, are difficult to determine on the basis of letters alone. Characteristics such as use of weapons or the occurrence of a description of the method were more concrete and verifiable. Emotions were categorized on the basis of Pennebaker (2011) and Chapman et al. (2009). According to Chapman et al. (2009) emotion words express feelings and desires, and negative emotions in particular, such as hatred and revenge, are associated with aggression. Pennebaker (2011) on the other hand wanted to demonstrate the relevance of linguistic markers, such as self-reference (I) and conjunctions in relation to self-awareness and deception. He posits that words like 'I' are an indication of state of mind and that self-reference and conjunctions are relevant because of the clues they contain regarding whether a person is telling the truth or not – which is also pertinent to the assessment of threatening letters. If these words are present in significant numbers, then they could be associated with future conduct. Which words, then, are related to repeat letter writing? And which words could serve as indicators that the letter writer will be arrested after having written the letter on suspicion of involvement in a violent act?

Examples of the method for making letter characteristics verifiable in the protocol are: threat classification (distinguishing between direct, conditional, indirect threat, or no threat), type of offence (violent offence, vandalism, possession of arms, assault, and other offences), form of the letter (handwritten, digital), addressing (Royal House, Prime Minister, Member of Parliament, other) and language use (emotion words, conjunctions, detailed information, self-reference). The protocol further operationalised abstract characteristics, such as burdened frame of mind, in questions such as: 1. The writer indicates being in pain and 2. The writer suffers from mental anguish as a result of personal loss. Using this method, more information could be obtained from the letters, and the verifiability of the letters was improved. The variables were coded as either present

(1) or absent (2). By coding the letters according to a protocol it was also possible to have the letters be assessed by two independent assessors[7] (Bijleveld, 2013), using Cohen's kappa statistic. A kappa of 1 (complete agreement) occurred for the characteristics: modi operandi (firearm, explosives, nuclear weapons), reference to own children, reference to spouse and reference to next of kin. A kappa of 0.75 – 1 (strong agreement) was found for the characteristics: distrust, confusion (conspiracy thinking), powerlessness, suicidal tendencies, threats, absence of modi operandi, reference to other persons, conjunctions, and terms abuse. A kappa of 0.4 – 0.75 (reasonable degree of agreement) was found for the characteristics: seeking justification, black and white thinking, exaggeration of events, incoherent language, emotional outburst, obtain concrete interests, defend acquired rights, revenge, cause fear, fixation, hatred, anger, personal loss/negative coping, pain, sacrifice one's life for a purpose, financial compensation, detailed information (location), prosocial engagement, positive coping, references to therapist, and use of uppercase/bold type. There were no characteristics that scored a kappa lower than 0.4. The sum of all calculated kappas divided by the number of known kappas resulted in a kappa of 0.74 (Appendix I). The characteristics for which the kappa could not be calculated, because they were too infrequent or entirely absent from the letters, were excluded in the data analysis. This also applied to characteristics with a kappa lower than 0.5, because this value is considered a less reliable score (Bijleveld, 2013). Some of the characteristics this applied to be: positive coping (seeking help) and prosocial engagement (offering help). The characteristic of 'negative coping' (personal loss, pain) was also excluded, because the inter-assessor reliability assessment revealed that there was an overlap with the characteristic of 'powerlessness'. The characteristic of 'powerlessness' also turned out to have a higher kappa than the characteristic of 'negative coping', which explains why only powerlessness was included in the analysis. Four of the eighteen characteristics that occur in Table I have therefore not been included in

[7] In order to establish inter-assessor reliability it was necessary that two other assessors assess the data. Two master's students in Forensic Criminology from the University of Leiden were asked to do this.

the analysis, either because the kappa was too low, or because the kappa could not be established. Consequently the model featured a total of 14 variables. The question that could have been asked here, was: which average reliability values were to be expected for certain combinations of assessor category type and knowledge of the instrument? The results show that those values were slightly higher for concrete letter characteristics (e.g. the occurrence of weapons, location, terms of abuse, uppercase type) than for a number of abstract characteristics, including the characteristic of 'remorse'. For the abstract letter characteristics the guidelines and operationalisations of the assessment framework were used, which also involved interpretation, experience, and knowledge (Baarda & De Goede, 2006). In practice this could mean not only those extra guidelines may be required for the way in which certain (abstract) letter characteristics ought to be interpreted, but also that knowledge and behavioural training for assessors are necessary.

In order to quantify the linguistic domains, the number of self-references (use of 'I') and the presence of conjunctions in the letters were counted. Conjunctions selected in the protocol included conjunctions of time (while), reason (because, as), restriction (except), purpose (so that), and condition (if, in case, provided that, unless). With regard to the occurrence of conjunctions, the assessment did not concern the combination of all these conjunctions, but rather whether the writer used any conjunctions in the letters. Self-references were divided into three groups in order to be able to compare the letters with each other: the number of self-references (use of 'I') in a letter were either in the first group (1 – 5), the second group (6 – 10) or the third group (11 – 15). This involved a relative step, created for that purpose, in which the number of self-references was counted for every ten lines. The development of the assessment framework and the drafting of the protocol (questionnaire) and the analysis of the letters took six months altogether.[8] All cases were documented, numbered, and processed in

[8] Aspects in the questionnaire – including gender, age, convictions, drugs, stalking – could not be verified adequately, if at all, in police systems, so these were not taken into consideration.

Statistical Package for the Social Sciences (SPSS),[9] version 19. This allowed for an anonymized analysis of letter writer data. SPSS was used to analyse the data quantitatively. The letters were analysed using bivariate and multivariate techniques (Lammers, 2007), and a chi-squared test was used for the descriptive analyses.[10] This test determined which relationships or differences existed between the characteristics of threatening letters and non-criminal threatening letters, repeated letters versus single letters, and whether or not the writer was arrested for a criminal offence. To assess which characteristics were decisive, a logistic regression analysis was applied for threatening letters, repeated letters, or committing a criminal offence.[11]

To summarise, the first step in the assessment of the kind of letters that this study is concerned with was the development of an assessment framework in which 18 (linguistic) characteristics are operationalised. This operationalisation used insights from forensic linguistics (Bogaerts, 2012; Dietz, 2010; Ekman, 1999; Vrij, 2010). In order to establish inter-assessor reliability the letters were assessed independently by two persons. Using SPSS version 19 the data was analysed using bivariate and multivariate techniques. The theoretical framework developed for this analysis constituted the guideline for a protocol (questionnaire) that improved letter assessment.

Results

The first finding was that direct threats were the most frequent (Table 2). Remarkably most letter writers address their letter to different public figures, and only a small group limited itself to addressing the Prime Minister or the Royal Family. Negative emotions, such as hatred, revenge, causing fear, and other factors, such as modi operandi and detailed information, were significantly associated with

[9] SPSS is a statistical computer program used for data collection, entry and analysis.
[10] The chi-squared test was used to establish whether letter characteristics were interrelated or significantly different from each other.
[11] Logistic regression analysis is used to establish whether there is a relationship between one dichotomous dependent variable and a number of independent variables. A dichotomous variable is a variable that can have only one of two values as output, for example 'yes' or 'no'.

the first group of letter writers that issue death threats, whereas fixation and confusion were significantly associated with the second group of non-criminal letter writers. This second group constituted half of this study, and requires the most care and attention from the authorities in charge of assessment, in view of the fact that they may require health care intervention. Fixation could play a role in carrying out an act (Meloy, 2001, 2011), which is what makes this second group, in addition to the threatening letters, highly relevant in terms of requiring constant assessment and monitoring. The frequent use of conjunctions proved significant only in the case of non-criminal threatening letters.

Table 2: Similarities and differences between threatening letters and non-criminal threatening letters (n=278 letter)

Threatened persons	*Threatening letters n=125*	*Non-criminal threatening letters n=153*	*$X^2(1)$*	*Cramer's V*
Prime Minister	20%	24%	.388	
Royal Family	14%	28%	.003*	.175
Other[12]	80%	62%	.538	
Type of letter				
Indirect threat	25%		.000**	1
Direct threat	49%			
Conditional threat	26%			
Details: Microfeatures and page lay-out features				
Handwritten	64%	73%	.126	
Digital	36%	28%		
Uppercase	43%	32%	.055	
Location and	19%	5%	.000**	.231

[12] This category applied when there was reference s to organisations, minister, state secretaries, and members of parliament or other politicians. The reason why the sum is greater than 100 per cent is because several individuals received letters from more than one writer.

numbers[13]				
Linguistic features				
Number of self-references	90%	84%	.258	
0-5	8%	14%		
6-10	2%	2%		
11-15				
Conjunctions[14]	47%	62%	.013*	.149
Background characteristics				
Cognitive distortion	67%	71%	.543	
Modi operandi[15]	54%	3%	.000**	.578
Incoherent language	75%	84%	.058	
Frame of mind, suicide	9%	15%	.115	
Fixation	6%	25%	.000**	.260
Confusion[16]	42%	73%	.000**	.320
Revenge	34%	13%	.000**	.253
Anger	50%	40%	.079	
Powerlessness[17]	9%	22%	.003**	.181
Cause fear	37%	0%	.000**	.493
Hatred	45%	9%	.000**	.418

The second analysis (Table 3, repeated letters) did not use the whole of the data file of letters (n=278), but only focused on those

[13] Location, time, date and numbers have been combined.

[14] For example: while, after, except, because, as, so that, if, in case, provided that, unless.

[15] Examples mentioned in letters: firearms, stabbing weapons, explosives and for example powder letters in which the substance often turned out to be washing powder or flour. The modi operandi percentage for the other letters indicates that instead of a treat the letter featured a desire for intimacy, involving a description of what the writer would like to do to get close to someone.

[16] For example conspiracy thinking, when the writer is convinced they are being followed or bugged.

[17] For example, the writer indicates not being able to solve their problems on their own, leading to feelings of powerlessness.

individuals that wrote both types of threatening letters, i.e. with and without criminal content (n=150). The analysis on repeated letters is, therefore, an analysis at an individual level, in order to avoid improperly counting writers that were responsible for repeated letters more than once. For repeated letters the characteristics of the first letter were considered. For this analysis only letters with a known date were used. This step eliminated 17 letters from the dataset, so that the test set was n=133.

In the group of repeated letter writers (Table 3) there were, in comparison with the group of one-off letter writers (49%), relatively many people sending letters in longhand (72%). A minority of the group writing more than one letter issued a direct threat (13%), which is in contrast to the writers of a one-off letter, among whom threatening letters (also with a direct threat) were much more common (35%). Furthermore, when compared to one-off letters, repeated letters differed significantly in terms of negative emotions such as fixation (18% vs. 4%) and confusion (72% vs. 35%). These emotions occurred significantly more in the letters by writers writing more than one letter, and they were for 69% non-criminal letters. To summarise, then, there are differences between individuals who write once and individuals who write more than one letter. For the latter group, this concerns the characteristics of 'confusion' and 'fixation'. This group also stands out for the fact that its letters are generally in longhand and non-criminal in their content.

Table 3: Characteristics associated with repeated letters (n=133 persons)

Threatened persons	*One-off letters n=94*	*Repeated letters n=39*	*$X^2(1)$*	*Cramer's V*
Prime Minister	20%	28%	.315	
Royal Family	20%	28%	.315	
Other[18]	72%	59%	.282	

[18] This category applied when there were reference s to organisations, minister, state secretaries, and members of parliament or other politicians. The reason why the sum is greater than 100 per cent is because several individuals received letters from more than one writer.

Type of letter				
Indirect threat	13%	10%		
Direct threat	35%	13%		
Conditional threat	15%	8%		
Non-criminal threatening letter[19]	37%	69%	.007**	.302
Details: microfeatures and page lay-out characteristics				
Handwritten[20]	49%	72%	.016*	.209
Digital	51%	28%		
Uppercase	30%	35%	.057	
Location and numbers[21]	16%	5%	.089	
Linguistic features				
Number of self-references	80%	87%	.600	
0-5	16%	10%		
6-10	4%	3%		
11-15				
Conjunctions[22]	48%	59%	.244	
Background characteristics				
Cognitive distortion	69%	77%	.366	
Modi operandi[23]	39%	18%	.017*	.207
Incoherent language	72%	77%	.585	

[19] On the whole, repeated letters were not threatening letters.

[20] The repeated letters were predominantly handwritten and to a lesser extent digital. This is a significant difference with one-off letters, where handwritten and digital letters were equal in numbers.

[21] Location, time, date and numbers have been combined.

[22] For example: while, after, except, because, as, so that, if, in case, provided that, unless.

[23] Examples mentioned in letters: firearms, stabbing weapons, explosives and for example powder letters in which the substance often turned out to be washing powder or flour.

Frame of mind, suicide	26%	13%	.106	
Fixation	4%	18%	.009**	.226
Confusion[24]	35%	72%	.000**	.335
Revenge	25%	18%	.413	
Anger	51%	41%	.292	
Powerlessness[25]	27%	21%	.460	
Cause fear	27%	8%	.015*	.211
Hatred	30%	21%	.273	

For the third analysis (Table 4) only those individuals (n=39) were selected that were arrested on suspicion of a criminal act after writing their first letter, and individuals (n=14) of whom it can be stated with certainty that they were not arrested for a criminal offence. Among the individuals arrested for a criminal offence, the emotion 'hatred' turned out to be significantly frequent (36% vs. 7%). For other negative emotions, however, no significant differences were found. Another significant characteristic that occurred more frequently for the group of writers arrested on suspicion of a criminal act in comparison to those that were not, is 'confusion' (67% vs. 36%). Also remarkable was the fact that the characteristics 'uppercase' and 'revenge' were not significantly more frequent by a small margin in the case of persons arrested on suspicion of a criminal act in comparison to persons who were not arrested. Contrary to expectation, fixation occurred less frequently with the group of arrested individuals (5% vs. 29%).

[24] For example conspiracy thinking, when the writer is convinced they are being followed or bugged.

[25] For example, the writer indicates not being able to solve their problems on their own, leading to feelings of powerlessness.

Table 4: Characteristics associated with being a suspect in a criminal offence (n=53 persons)

Threatened persons	*Not a suspect n=14*	*Arrested for criminal offence n=39*	*$X^2(1)$*	*Cramer's V*
Prime Minister	14%	33%	.175	
Royal Family	50%	33%	.270	
Other[26]	43%	58%	.807	
Type of letter				
Indirect threat	7%	15%	.766	
Direct threat	22%	21%		
Conditional threat	7%	13%		
Non-criminal threatening letter	64%	51%		
Details: micro features and page lay-out characteristics				
Handwritten	50%	64%	.355	
Digital	50%	36%		
Uppercase	14%	42%	.061	
Location and numbers[27]	14%	5%	.266	
Linguistic features				
Number of self-references	93%	74%	.335	
0-5	7%	23%		

[26] This category applied when there were reference s to organisations, minister, state secretaries, and members of parliament or other politicians. The reason why the sum is greater than 100 per cent is because several individuals received letters from more than one writer.

[27] Location, time, date and numbers have been combined.

6-10	0%	3%		
11-15				
Conjunctions[28]	71%	62%	.508	
Background characteristics				
Cognitive distortion	79%	82%	.775	
Modi operandi[29]	29%	23%	.682	
Incoherent language	79%	90%	.290	
Frame of mind, suicide	21%	21%	.942	
Fixation	29%	5%	.018*	.326
Confusion[30]	36%	67%	.044*	.277
Revenge	7%	33%	.057	
Anger	43%	51%	.589	
Powerlessness[31]	21%	28%	.622	
Cause fear	7%	8%	.947	
Hatred	7%	36%	.040*	.281

Logistic regression analysis (Table 5) was then used to investigate which characteristics in letters were risk-increasing, which made it possible to select for repeated letter writers and for individuals who would later be arrested on suspicion of a criminal offence, such as assault. For this analysis only the independent variables – i.e. predictor variables – were used in the model. The independent variables are from the categories 'background characteristics' and 'linguistic characteristics' (Table 1). The dependent variables are: threat yes/no,

[28] For example: while, after, except, because, as, so that, if, in case, provided that, unless.

[29] Examples mentioned in letters: firearms, stabbing weapons, explosives and for example powder letters in which the substance often turned out to be washing powder or flour.

[30] For example conspiracy thinking, when the writer is convinced they are being followed or bugged.

[31] For example, the writer indicates not being able to solve their problems on their own, leading to feelings of powerlessness.

repeated letter yes/no, arrest on suspicion of criminal offence yes/no. For repeated letters (n=133) and for individuals arrested on suspicion of a criminal offence (n=53) the data sets were used that also served for the bivariate analyses. Because the model consists of a fair amount of independent variables (14)[32], for the first regression analysis for threat Cronbach's Alpha (α) was applied first to establish whether a number of variables could be collected in a single scale, in order to make the model better testable. From this test it emerged that the Cronbach's Alpha value for 'hatred-revenge' was α=0.653. For 'frame of mind-powerlessness' the value was α=0,656. This justified limiting the model (number of characteristics) for threat (going from 14 to 12 characteristics), by turning 'hatred-revenge' and 'frame of mind-powerlessness' respectively into two new scales.[33] In order to assess whether the threat contained in the first letter could also be a predictor for repeated letters, 'threat' was then used as a characteristic for the second regression analysis for persons that wrote more than one letter, so that the model (in the second column) used for testing counted 13 characteristics (instead of 12). For the analysis of repeated letters yes/no, again only the characteristics of the first letter were used. For the final regression analysis (third column) both the factors of 'threat' and 'repeated letters' were added to the model for being arrested on suspicion of a criminal offence. The goal here was to investigate whether these characteristics would improve the model, so that consequently the model for the third column counted 14 characteristics. Contrary to the first two regression analyses, which consisted of fairly large data sets (n=278, n=133), the method for this test was more exploratory and the forward Wald selection test was applied because the data set was considerably smaller (n=53) and the results were difficult to interpret as a result of multicollinearity.[34] Using

[32] Characteristics with kappa lower than 0.5 were excluded from the analysis.

[33] For the other characteristics, the Cronbach's Alphas were lower than 0.450 and for that reason too unreliable for constituting new scales as well.

[34] Multicollinearity is a statistical phenomenon in which two or more predictive variables in a regression model show strong correlation, which means that at least one of them can be predicted on the basis of the model. Multicollinearity influences the calculation of coefficients, because in such cases the characteristics overlap at least partially.

the forward Wald selection test it was then tested in three steps which characteristics in this model were important (Lammers, 2007). In other words, the independent characteristics were added one by one, and for each it was tested whether the addition improved the model. This explains why the third column in Table 5 is relatively sparsely populated, which is due to the different selection procedure used for this test and the fact that the smaller data set used was the more accurate one. As a result this column contains only those characteristics for which tests have shown that they are significant predictors. The characteristics 'hatred-revenge' and 'confusion' in particular are significantly associated with the chance of being arrested on suspicion of a criminal offence. In addition, the characteristic of 'fixation' turned out to be less associated with those that were later arrested on suspicion of a criminal offence (Exp (B) <1). In the other analyses (Table 2, 3) fixation appeared mostly in connection with non-criminal threatening letters and with repeated letters. Furthermore the characteristic of 'confusion' turned out to be an important predictor for whether a letter writer would resort to writing more than one letter.

Table 5 Regression analyses: threatening letters, repeated letters and arrest for criminal offences

	Threatening letter (n=278)		Repeated letter (n=133)		Arrest for criminal offence (n=53)	
Background characteristics	Exp (B)	Sig.	Exp (B)	Sig.	Exp (B)	Sig.
Cognitive distortion	,804	,594	1,127	,849		
Modi operandi	22,139	,000**	1,125	,870		
Incoherent language	1,515	,376	,584	,360		
Fixation	,520	,236	1,190	,823	,075	,025*
Confusion	,399	,014*	3,177	,034*	13,529	,005**
Hatred-revenge	5,521	,001**	1,400	,622	20,038	,032*

Anger	1,253	,539	,640	,403		
Powerlessness/ Frame of mind	,213	,018*	,335	,144		
Cause fear[35]			,414	,331		
Linguistic features						
Number of self-references	1,258	,583	,542	,262		
0-5						
6-10						
11-15						
Conjunctions	,700	,300	1,181	,727		
Details[36]	2,583	,012*	1,120	,806		
Added predictor variables[37]						
Threat			,307	,051		
Repeated letter						
Constant	,633	,777	3,067	,672	,031	,151
Nagelkerke R Square		,541		,293		,445
N		278		133		53

Conclusion and discussion

For persons who were arrested on suspicion of a criminal offence, this study has shown that the characteristics of 'hatred-revenge' and 'confusion' are predictor variables for these threateners.

[35] The characteristic of 'cause fear' was difficult to calculate because of overlap with other coefficients. For that reason it was removed from the model so that the total number of characteristics in that column is 11 instead of 12.

[36] For the purpose of this analysis only microfeatures were assessed, including: uppercase, location, time, date, and numbers.

[37] For repeated letters in the second column the characteristic of 'threat' was added to the regression analysis as an independent variable in order to determine whether this characteristic might be significantly associated with repeated letter writing. For arrest for criminal offence the characteristics of 'threat' and 'repeated letter writing' were added. Both characteristics turned out not to be significantly associated with repeated letter writing and arrest for a criminal offence.

This result – the most important results of the regression analyses – can be used for selection purposes when assessing threatening letters and non-criminal threatening letters. The characteristic of 'confusion' is a relevant predictor variable to indicate whether someone will write more than one letter, and the characteristics of 'confusion' and 'hatred' together contribute to the chances that someone will be arrested in the future on suspicion of a criminal offence, such as assault.

This study referred to Pennebaker (2011) to interpret the relevance of conjunctions, detailed information and self-reference. In Pennebaker's theory, self-reference, detailed information and conjunctions are associated with exposing violent intentions. Conjunctions (non-criminal threatening letters) as well as detailed information (threatening letters) occurred significantly more often in the letters, but in follow-up analyses only the aspect of detailed information persisted as a factor in threatening letters.

Contrary to expectation, fixation turned out to be uncorrelated with threatening letters or to individuals arrested on suspicion of a criminal offence. In Meloy's theory (2001, 2011) fixation could play a role in carrying out an act. In the descriptive analyses, fixation was perceived as a significant characteristic in non-criminal threatening letters. Non-criminal threatening letters were mostly found with persons who wrote more than one letter, and who also significantly featured the characteristic of 'confusion'. This second group constituted half of this study, and requires the most care and attention of the authorities in charge of assessment, in view of the fact that they may require health care intervention. In the case of the descriptive analyses the characteristic of 'powerlessness' also turned out to occur significantly with writers of non-criminal threatening letters. Possibly, but this is hypothetical, for this group this characteristic is a contributing reason for writing letters repeatedly. Future research should therefore try to examine repeated letters for possible observable changes in the writer's frame of mind between the first and the follow-up letters. The characteristics of 'hatred-revenge' and 'confusion' emerged from the regression analyses of this study as the most strongly and significantly correlated with the chances of arrest on suspicion of a criminal offence. For repeated letters this characteristic proved to be

'confusion. These aspects persisted in the regression analyses and they may be relevant for the assessment of repeated letters and for individuals arrested on suspicion of a criminal offence. In the first place the aspect of confusion was found to be a significant predictor variable in 72% of repeated letter cases. Confusion also emerged in the descriptive studies of threateners, e.g. Fein et al. (1999), in which this aspect was found to be a possible match between threateners and perpetrators of violence. Fein et. al. based themselves on the personal backgrounds – available for threateners and for almost half of the perpetrators of violence – of those who carried out an attack on a public figure in the US in the past. Confusion was also present as a characteristic in a study of threatening letters addressed to the Dutch Royal Family (Van der Meer et al., 2012). The major part of letter writers examined in this study turned out to be known to or undergoing treatment at psychiatric clinics or other care institutions. The fact that confused letter writers may have a history with health care providers was also shown in a study into threats against the British Royal Family by James et al. (2009). According to the researchers, 80% of the tested individuals appeared to suffer from a psychiatric disorder, such as depression, psychosis, and schizophrenia, sometimes in combination with other factors like substance abuse and past violent behaviour.

The regression analyses also showed that acknowledging hatred or revenge as a motive for the letter correlates with a heightened chance of arrest on suspicion of a violent offence, which is in agreement with the theory of Chapman et al. (2009). The function of hatred is to rule out or eliminate certain objects, and in the literature it is seen as a dangerous emotion (Chapman et al., 2009; Ekman, 2008; Levenson, 2003). Hatred can be viewed as a moral emotion that is intrinsically motivating, i.e. there is a possible link between moral emotions and the motivation for action.

It may be appropriate to account for differentiation in these results. The personal circumstances of a threatener can change, and both internal and external changes can influence the question whether a threatener will send another email or letter. A threatening letter may have been written as the result of a particular combination of time and a set of circumstances, and the same caveat applies to the assessment of

a threatening letter's risk. Risk assessment is dynamic, and sometimes requires a renewed assessment when a repeat letter occurs (Jopeck, 2000). Although it was possible in this study to show for a small group whether, after writing a letter, an arrest on suspicion of a criminal offence like assault took place, it did not consider whether this action was directed at a public figure. The reason for this can be found in the focus of the study. The assault, for which someone may have been arrested, could also have been directed at someone who is not in the public eye. A study by Smith (2006) shows that a threatener often takes a course of action that is different from the one announced in the letter, or chooses a different person or object that is relatively unprotected or vulnerable. Not only assessors, but also security officials should be aware of the fact that writers of threatening letters could also target persons or objects that are not protected. Still, this study adds to the available knowledge regarding the phenomenon of threatening letters, in particular in the finding that non-criminal letters may require the most time and/or attention because of the possibility of repeated letters (69%). More than criminal threatening letters, this category also requires the most care and attention of the assessing authorities, in view of the fact that they may require health care intervention.

Recommendations

The first recommendation concerns the police and other organisations in the field of security: the characteristics identified in this study provide a procedural aid for the collection of information or for investigation. In theory the assessment is restricted to providing an estimation of the characteristics, so that it provides a cue for further investigation in order to arrive at a well-considered judgement. To that end it is important that also other available information can be requested, in order to create a case file.

The second recommendation has to do with organisations that work with largescale data or detection programmes. The digitalisation of society requires different ways of thinking and acting if threateners are to be identified at an early stage. The communication techniques of threateners change, and this requires innovative methods for practical efficient methods for data assessment. It is quite possible that detection

programs lack some of the nuances of a human approach, but testing for characteristics such as 'hatred-revenge' and 'confusion' could also be applied to large data files using the assessment protocol developed to that end. What is relevant here, is that assessors have complete access to all necessary information, and data analysis on deviant behaviour will contribute to this.

Recommendation three: make the methodology for assessing threatening letters a part of the training of assessors who as part of their work have to assess and process such letters on a day-to-day basis.

The fourth recommendation is for those that are threatened: file a police report. In order to have a clear view of the threats directed at politicians it is important that public figures report threats to the police. The reason for this is because the number of threats directed at public figures is much larger than the number of filed reports. The possibility of monitoring threats using a database would also provide insight into how frequent and over which extended period some threateners have been issuing threats.

The fifth recommendation is concerned with follow-up research intended to generalise the results of this study and apply them to the decentralised domain (civilians). In order to be able to generalise the results externally also to a larger group, it is advisable to repeat the study for external validation in the decentralised domain, such as local administrative authorities. This will also make it possible to investigate whether the characteristics in the assessment table show a certain degree of consistency (or pattern) that could also apply to larger groups of threateners that have been arrested on suspicion of offences (Bateman & Salfati, 2007). Furthermore this study noted frustration-aggression or emotional aggression in particular in the case of direct threats, with references in the threatening letter to an external provocative event that constituted the trigger for the letter and that expressed itself as causing fear (Kemper & Ruig, 2009). In the case of conditional threats also instrumental aggression was noted, wherein certain conditions were attached to obtaining a goal. More so than emotional aggression, instrumental aggression may be connected to action. Hypotheses that could be examined in follow-up studies, could include: (1) from which of these two groups was a perpetrator later

convicted for offences like assault, and (2) which rational conduct preceded the violence in order to, for example, obtain emotional benefit (Kruize & Wijmer, 1994)?

The sixth and final recommendation concerns fixation and creating a timeline. The characteristic of fixation was most frequent in this study in the case of repeated letters and in non-criminal threatening letters. In the literature fixation is associated with violent behaviour and it is a characteristic that overlaps with stalking (Brandt, 2012), with a pattern of harassing and disturbing letters, emails, or packages that are perceived by the person being threatened as frightening (MacKenzie, et al., 2009; Rugala et al., 2004). Repeated letters are therefore very relevant for follow-up studies, also from the point of view of the person being harassed; these letters will, after all, have an impact on the social and private life of someone being threatened. In those letters the characteristic of fixation was most frequent, in addition to the non-criminal threatening letters. The frequency of threatening communications by someone can be plotted on a timeline that provides insight into the progress and contents of the communications (Van der Meer & Diekhuis, 2013). A timeline can be used to map changes in frame of mind or language use. A first contact could, for example, develop out of frustration or a disorder and eventually result in a specific threat directed at a politician or other public figure. A follow-up study could focus on the characteristics of the second threatening letter and any other letters written by the same person, and compare the results.

References:

1. Baarda, D.B. & De Goede, M.P.M. (2006). Basisboek Methoden en technieken. Handleiding voor het opzetten en uitvoeren van kwantitatief onderzoek. Noordhoff Uitgevers B.V.

2. Bateman, A.L. & Salfati, C.G. (2007). An examination of behavioral consistency using individual behaviors or groups of behaviors in serial homicide. *Behavioral Sciences and the Law*, 25, p. 527 – 544.

3. Bogaerts, S., Okur, P., Willems, M., Knaap, L. van der, Spreen, M. Aertsen, I. (2012). *Solistische dreigers. Ontwikkeling van een instrument voor*

risicotaxatie van solistische dreigers. School of Behavioral Sciences: Tilburg University.

4. Bijleveld, C.C.J.H. (2013). Methoden en technieken van onderzoek in de criminologie. Den Haag Broom Criminologie.

5. Bovenkerk, F. (2005). Bedreigingen in Nederland, Willem Pompe Instituut. Universiteit Utrecht.

6. Brandt, C. & Voerman, B. (2012). Checklist bij stalking. www.klpd.politie.nl.

7. Canter, D. (2000). Offender profiling and criminal differentiation. *Legal and Criminal Psychology, 5,* p. 23 – 46.

8. Chapman, H.A., Kim, D.A., Susskind, J.M. & Anderson, A.K. (2009). In Bad Taste: Evidence for the Oral Origens of Moral Disgust. *Science 323,* p. 1222 – 1226.

9. De Groot, I.N.J., Drost, L.F., Boutellier, J.C.J. (2009). *Bedreigers van politici. Risico's en interventiemogelijkheden.* Verwey Jonker Instituut, Utrecht.

10. De Vocht (2011). SPSS 19. Bijleveld Press.

11. Dietz, P.E. (1991a).Threatening and otherwise inappropriate letters to Hollywood Celebrities. *Journal of Forensic Sciences* 36, p. 185 – 209.

12. Dietz, P.E. (1991b).Threatening and otherwise inappropriate letters to members of the United States Congress. *Journal of Forensic Sciences*, 36, p. 1445 - 1468.

13. Dietz, P.E., Mattews, D.B., Martell, D.A., Stewart, T.M., Hrouda, D.R., & Warren, J. (1991). Threatening and otherwise inappropriate letters to members of the United-States-Congress. *Journal of Forensic Sciences*, *36,* p. 1445 – 1468.

14. Dietz, P.E., & Martell, D.A. (2010). Commentary: Approaching and Stalking Public Figures. A Prerequisite to Attack. *Journal of the American Academy of Psychiatry and the Law, 38,* p. 341 – 348.

15. Ekman, P. (1999). Basic emotions. In T. Dalgleish & T. Power (Eds.), *The handbook of cognition and emotion (*p. 45 – 60*).* Sussex, United Kingdom: John Wiley and Sons, Ltd.

16. Fein, R. A., & Vossekuil, B. V. (1999). Assassination in the United States: An operational study of recent assassins, attackers, and near-lethal approachers. *Journal of Forensic Sciences*, 44, p. 321 – 333.

17. James, D.V., Mullen, P.E., Pathe, M.T., Meloy, J.R., Preston, L.F., Darnley, B., Farnham, F.R. (2009). Stalkers and harassers of the royalty: the role of mental illness and motivation. *Psychological Medicine*, *39,* p. 1479 – 1490.

18. James, D.V. (2010). Protecting the prominent? A research journey with Paul Mullen. *Criminal Behaviour and Mental Health*, 20, p. 242 – 250.

19. James, D.V., Meloy, J.R., Mullen, P.E., Pathe, M.T., Farnham, F.R., Preston, L.F., & Darnley, B.J. (2010a). Abnormal Attentions Toward The British Royal Family: Factors Associated With Approach and Escalation. *Journal of the American Academy of Psychiatry and the Law*, 38, p. 329 – 340.

20. James, D.V., McEwan, T.E., MacKenzie, R.D., Meloy, J.R., Mullen, P.E., et al. (2010). Persistence in stalking: A comparison of associations in general forensic and public figure samples. *Journal of Forensic Psychiatry and Psychology,* 21, p. 283 – 305.

21. James, D.V., MacKenzie, R.D., Farnham, F.R. (2014). The Communications Threat Assessment Protocol (CTAP-25). *Intelligence, 2*.

22. Jopeck, E. J. (2000). Five steps to risk reduction: Learn to identify and reduce risk by following these five steps. *Security Management*, 44 (8), p. 97 – 98, p. 100 – 102.

23. Kemper, R., & Ruig, L. de (2009). Tussen agressiebeleid en praktijk: *Aanpak van agressie en geweld in de publieke sector.* Zoetermeer: Research voor Beleid.

24. Kruize, P., & Wijmer, D. P. (1994). Geweldsincidenten tussen politiemensen en burgers in Den Haag. *Justitiële Verkenningen*, 20(1), p. 97 – 112.

25. MacKenzie, R.D., McEwan, T.E., Pathé, M.T., James, D.V., Ogloff, J.R.P., Mullen, P.E. (2009). *The Stalking Risk Profile. Guidelines for assessing and managing stalkers.* StalkInc. & the Centre for Forensic Behavioural Science: Monash University.

26. Meloy, J. R. (2000). *Violence Risk and Threat Assessment*. A Practical Guide for Mental Health and Criminal Justice Professionals. San Diego, California: Specialized Training Services.

27. Meloy, J.R. (2001). Communicated threats and violence toward public and private Targets: discerning differences among those who stalk and attack. *Journal* of Forensic Sciences, 46, p. 1211 – 1213.

28. Meloy, J.R., James, D.V., Farnham, F.R., Mullen, P.E., Pathe, M., Darnley, B., Preston, L. (2004). A research review of public figure threats, approaches, attacks, and assassinations in the United States. *Journal of Forensic Sciences, 49,* p. 1086 – 1093.

29. Meloy, J.R. (2007). Antisocial personality disorder. *In G.O. Gabbard (Ed.), Treatments of psychiatric disorders.* Washington, DC: American Psychiatric Publishing, 4th ed., p. 2273 – 2290.

30. Meloy, J.R., Sheridan, L, Hoffmann, J. (2008). Stalking Threatening, and Attacking Public Figures. A Psychological and Behavioral Analysis. Oxford University Press.

31. Meloy, J.R., James, D.V., Mullen, P.E., Pathé, M.T., Farnham, F.R., Preston, L.F., Darnley, B.J. (2011). Factors Associated with Escalation and Problematic Approaches Toward Public Figures. *Journal of Forensic.*

32. Pennebaker, J.W. (2011). The secret life of pronouns. What our words say about us. New York: Bloomsbury Press.

33. Rugala, E., McNamara, J., & Wattendorf, G. (2004). *Expert Testimony and Risk Assessment in Stalking Cases. The FBI's NCAVC as a Resource.* In FBI Law Enforcement Bulletin, p. 8 – 17. Washington, D.C.: U.S. Department of Justice.

34. Van der Meer, B.B., Bootsma, L., Meloy, R. (2012). Disturbing Communications and problematic approaches to the Dutch Royal Family. *The journal of Forensic Psychiatry & Psychology, 1 – 19, iFirst* article.

35. Van der Meer, B.B., & Diekhuis, M.L. (2013). Collecting and Assessing Information for Threat Assessment. In R. Meloy & J. Hoffmann (Eds). *International Handbook of Threat Assessment, part I, 3.* New York: Oxford.

36. Voerman, B. E. & Brandt, C., Bullens, A.R. (2014). Stalking Risk Profile: richtlijnen voor Risicotaxatie en Management van Stalkers. Utrecht: Studio S & H.

37. Vrij, A. (2010). *Detecting Lies and Deceit(2nd ed.).* Pitfalls and Opportunities. Chichester: John Wiley & Sons, Ltd.

Appendix[38]

Cohen's Kappa

Name of variable	**Cohen's kappa**
Cognitive distortions justification	.618
Cognitive distortions black-and-white thinking	.645
Cognitive distortions distrust	.759
Cognitive distortions exaggeration of events	.731
Incoherent language	.696
Emotionel outburst	.673
obtain concrete interests	.641
defend acquired rights	.67
Revenge	.587
Cause fear	.718
Fixation	.628
Confusion	.806
Social isolation	X
Unknown	X
Hatred / revulsion	.689
Anger	.694
Powerlessness	.932
Personal loss / negative coping	.602
Pain*	X
Pain / hurt	X
Pain / sacrifice one's life for a purpose	.494
Burdoned frame of mind or suicidal	.936

[38] Note: the X in the table indicates that SPSS was unable to calculate the kappa, because the variable was a constant. The variable pain (hurt) for example, was not observed in the letters by either assessor 1 or assessor 2, and both scored this aspect as 'absent'. Some characteristics were operationalized as sub characteristics in order to improve their measurability, such as cognitive distortions, modi operandi, and references to other persons, negative coping, positive coping, and anger. This explains the number of characteristics. For the characteristic of 'self-reference' ('I') no kappa was calculated, instead counting the number of self-references for each ten lines of the letter. Consequently, a kappa was only calculated for nominal or categorical variables.

tendencies	
Remorse	X
Threats	.817
Media threat	X
Financial compensation	.628
Location	.642
Date	X
Time	X
Numbers	X
Modus operandi firearms	1
Modus operandi stabbing weapon	X
Modus operandi explosives	1
Modus operandi nuclear weapons	1
Modus operandi vice	X
Modus operandi other	.73
Modus operandi absent	.801
Prosocial engagement	.401
Positive coping	.482
Reference to parents	X
Reference to siblings	X
Reference to other next of kin	X
Reference to own children	1
Reference to spouse	1
Reference to friends	X
Reference to psychiatrist	X
Reference to therapist	.656
Reference to other close persons	1
Reference to other persons	.909
Conjunctions	.802
Terms of abuse	.845
Uppercase / bold	.703

CASE STUDIES INTO THE UNKNOWN – LOGIC & TOOLING

Giliam DE VALK*

Abstract

Case study is the most common method in intelligence research. Intelligence analysis takes place in a context of denial and deception by opponents that also constantly innovate themselves. In that context, the analyst does not want to miss threats.

Can a research design on threats be structured such that less relevant relationships are missed? In methodological terms: to reduce the value of the β. A tool is presented in which different types of unknowns are distinguished, in which either the data or the technique to retrieve those data are unknown. In this tool – the Rumsfeld Matrix – both the quantitative and qualitative approach is integrated. Also, all three types of logic – abduction, deduction, and induction – can be applied. Thus, the change of missing relevant relationships on threats is reduced.

Next, a model is presented to assess what is covered in a case study in terms of logic. It is tool to organize and evaluate your case research. Through this Standard Logic Model it can be visualized what the current coverage of a case is, and what the desired state would look like. It is also assessed what techniques will cover what part of a case. It integrates three aspects. Firstly, all three forms of logic are included. Secondly, it combines both the qualitative and quantitative approach. Thirdly, analysis by humans and analysis by machines is combined. It will lead to an enhanced way of working – that of augmented analysis in which humans and machines are paired in their analytic effort.

Keywords: *β, unknown, tooling, Rumsfeld Matrix, logic.*

Introduction

In this article, it is dealt with case studies into the unknown. In the context of intelligence, dealing with the unknown tends to be more complex than in other disciplines as denial and deception are endemic.

* Assistant Professor Phd at the Institute for Security and Global Affairs, University of Leiden, email: g.g.de.valk@fgga.leidenuniv.nl

Also the nature of the threat will evolve as opponents are constantly innovating themselves.

How do you draft a case study in such a context? Firstly, a tool is presented that deals with different types of unknowns that have to be investigated. Secondly, another tool is presented to assess to what extent the complete picture of the case at hand – a so-called C-theory – has been covered, and to what extent it deals with possible future innovations by an opponent. Both aspects will be visualized in one scheme in which an ordinal – not absolute – impression is given of what has been covered.

The two tools are aimed to be of practical use for the intelligence practitioner. The practitioner can make assessments and design policies to cope with future developments. At an academic level, it points at methodological issues to be addressed. It can help to organize academic teaching and research around methodological issues and practices.

The focus is on threat related intelligence case research into the unknown. The tools will be illustrated with examples of preparing a Peace keeping Operation (PKO). But first, it will be dealt with some basic methodological insights.

Case-theory, α and β

Academics usually understand theory as a general or nomothetic theory. A phenomenon is explained in a general sense. This type of theory is referred to as a level-A theory (De Groot, 1981). Practitioners also develop a theory, but in the form of a level-B and level-C theory. The level-B theory is a problem oriented special theory, and limited to a certain category of cases. The level-C theory is developed for an individual case. This is also referred to as an idiom theory (Van Strien, 1986).

The level-C theory – or Casus-Theory – is used by intelligence practitioners to analyze a concrete case. It is aimed at actions concerning future situations, and not at scientific theory. It is primarily aimed at interventions – to achieve a situation that is believed to be the desired one. This is contrary to scientific research that is primarily aimed at truth finding. By that the object of intelligence research is more *mutandum* than *explanandum* (Van Strien, 1986).

But how do we use a C-theory in intelligence analysis? There are high quality publications on case-study research, as by Robert Yin (Yin, 1994), but they are not calibrated to the specific methodological needs of applied intelligence research. His publication is written for scientific purposes in order to explain. Intelligence is, however, in the first place aimed at not to miss threats. This is complex as denial and deception, and future innovations by an opponent are characteristic for this type of research. The aim of intelligence is to give warnings to avert a threat. This difference in setting and orientation leads to a different methodological approach of intelligence case research, compared to other methods.

To explain versus not miss are central in some basic methodological terminology. To explain is related to the α (and Type I error). Not to miss is related to the β (and Type II error). The α is the chance that you *incorrectly* conclude that there is a significant relationship between phenomena (a Type I error means accepting a hypothesis when in reality this hypothesis is false). The β is the chance that you *do not discover* a weak, but actual existing, relationship between phenomena (a Type II error consists of rejecting a 'true' hypothesis).

In academic research, the emphasis is on to reduce the α – the chance that you incorrectly conclude that there is a significant relationship between phenomena. In intelligence research, however, the emphasis is primarily on not to miss a threat – the β – the chance that you do not discover a weak, but actual existing, relationship between phenomena. To put it in plain language: in intelligence it is often more critical that you do not miss a threat (β orientated research), than that you scientifically prove or explain that a threat will occur (α orientated research). This calls for a research design, and the application of logic, methods and techniques, with respect to their β capabilities (De Valk, 2011).

Although the emphasis is on the β, the issue of the Type I error is not to be excluded from intelligence research. The intelligence equivalence of the Type I error is to err on the side of caution. For example, this implies overestimating the enemy's capabilities. Concerning the Type II error, scientists may ignore or discount the

significance of these errors in their studies. However, intelligence analysts do not have this luxury. Thus they are confronted by these two simultaneous pressures that require them to minimize both types of error simultaneously. Therefore, the calibration process of intelligence assessments is far more demanding than scientific calibration, and the likelihood of mistakes is higher (Goldbach, 2012). It calls for research design tools that are related to both errors – the α and the β.

Secrets, puzzles, and mysteries, and Structured Analytic Techniques

In intelligence, case studies will differ in complexity. The tools that will be presented in this article are meant for the more complex ones, that Treverton called puzzles and mysteries (Treverton, 2009). A problem with data in those complex case studies is that the noise can obscure the signal – including the issue of overfitting (Silver, 2012). The more complex a problem is, the less favorable will be the relationship between the data in terms of noise and signal (Menkveld, 2018). To reduce the change of biases in such situations – as for puzzles and mysteries – the analyst has to rely on tooling and multiple Structured Analytic Techniques, or SAT's (Moore, 2011. Menkveld, 2018). But how do you arrange your SAT's to assess as accurate as possible (to reduce the value of the α), and at the same time not to miss a threat (to reduce the value of the β)? First, it is dealt with the tooling to reduce the value of the β (Rumsfeld Matrix), and then the focus is on the overall research design in terms of logic (Standard Logic Schedule).

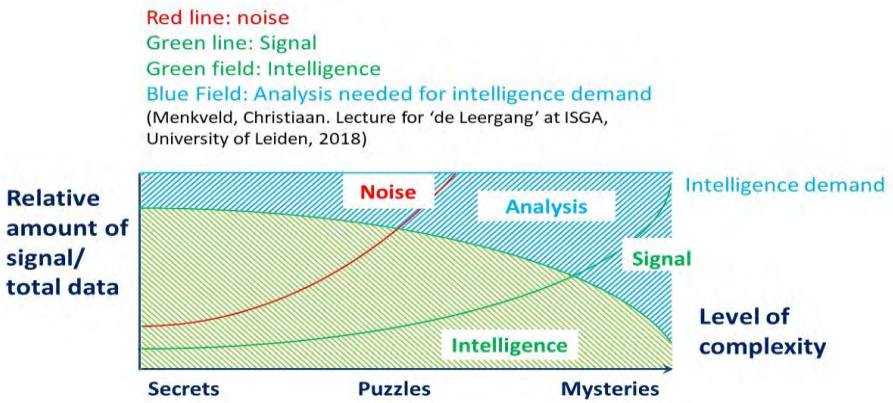


Figure 1: The relationship between the data in terms of noise and signal (Source: Menkveld, 2018)

Rumsfeld Matrix: How not to miss a threat?

There are no manuals on a β research design. Some publications concern β-aspects, for example when they deal with techniques as Quadrant Crunching, Red Team, Red Cell or Alternative Analysis (as in Heuer/Pherson, 2011; *Red Team Handbook*, 2012). However, the β research design itself remained a blind spot. In the Netherlands, some initiatives were taken by Onno Goldbach and Giliam de Valk to explore the possibilities of such a β research design. As a starting point a statement by Donald Rumsfeld was taken. In 2002, the then United States Secretary of Defense, Rumsfeld stated:

> [T]here are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – there are things we do not know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones (U.S. DoD, 2002).

A Rumsfeld Matrix derived from what he said that day, has been used more often. However, the Rumsfeld Matrix had never been used for a methodological arrangement of the β capabilities until 2013. The composition of such a β research design is since 2013 part of the Minor Intelligence Studies, first at the University of Amsterdam (Ad de Jonge Centre) and, since 2017, at the University of Leiden (ISGA). This subsection on the Rumsfeld Matrix is a reworked version of De Valk, 2018. Starting point was to distinguish between different types of unknowns – whether the way to *retrieve* data is known or not, and whether these *data* themselves are known or not. It leads to four combinations of *retrieval* and *data*. Each of those combinations is a quadrant of the matrix, and refers to a certain combination of elements that you may miss. Each quadrant covers a part of the puzzle of the [un-]known-[un-]known, and is part of the research design to reduce the value of the β as much as possible. If his statement is thus rearranged in a matrix, it results in the following composing elements of, for example, a Peace keeping Operation (PKO) mission (the mentioned techniques will be explained later in this article):

PKO	KNOWN	UNKNOWN
KNOWN	Critical Thinking	Early Warning & Critical Indicator Driver Based Scenario Building
UNKNOWN	Data Science Cell	Red Cell & Red Reaming

Figure 2: The Rumsfeld Matrix: data and retrieval
PKO arrangement for near term early warning and mid-term policy planning
(Source: The Rumsfeld Matrix is a reworked version of De Valk, 2018)

Known-Known

In the *Known-Known* quadrant, both the technique to obtain the data [*retrieval*] and the *data* are known. The known-known quadrant refers to the contents of assumptions, information, and knowledge of which we know that we know them. In general, this quadrant is about

challenging: are you really sure about what you think that you know, that you know?

For a PKO, for example, an *Early Warning and Critical Indicator (EWCI)* system is vital to warn on the near term. Within such an *Early Warning and Critical Indicator* system you need to check if the so-called Critical Indicators of a Warning Scenario are still accurate (*Known-Known*). The accuracy of a Critical Indicator is vital because it then will provide an accurate warning in case of threats (EAPC, 2001).

Known-Unknown

In the *Known-Unknown* quadrant, the technique of *retrieval* is known, but the *data* themselves are unknown. In a PKO, for example, you are aware that a threat is present, but the exact possible courses of action are unknown. In order not to miss threats, methods and techniques are used. In the context of a PKO, for example, *Driver Based Scenario Building (DBSB)* can be used for mid and long term policy planning. The likelihood of the different scenarios is monitored by collecting data for the indicators that are formulated for each scenario. The *data* are not available yet, but the technique of *retrieval* is known (scenario building, including the formulation of indicators).

Unknown-Known

In the *Unknown-Known* quadrant, the technique or algorithm to obtain data [*retrieval*] is unknown, but the *data* as such are present. It is about, for example, finding relevant correlations by big data-analyses. In intelligence, tooling is developed for, among others, data mining, criminal profiling, geographic profiling, spatial analysis, social network analysis, SOCMINT and GEOINT. The quantitative part can be automated in so-called Data Science Cells, who will play a major role in a PKO to get a grip on the developments.

Unknown-Unknown

In the *Unknown-Unknown* quadrant, both the technique to obtain data [*retrieval*] and the *data* are unknown. This is a difficult quadrant to deal with. Not only because it is hard to reflect on things you do not know of, but also because there are just a few techniques developed to

detect unknown-unknowns. These techniques mainly take the form of an experiment. In such an experiment a group of persons is asked to carry out an authorized attack on their own organization, to see if something is overlooked. Such an experiment is often referred to as Red Team or Red Cell. Red Teaming is not limited to the opponents' perspective, but can also include the broader scope of society itself, including secondary and tertiary effects (*Red Team Handbook*, 2012). Based on the results of Red Team and Red Cell experiments, security measures are taken. The outcome of a PKO Red Cell experiment can be that insurgents may, for example, adapt *satellite patrol* – in which this patrol intentionally separates itself visually and physically from the base unit of the patrol, outside the visual contact (*Urban Operations III*, 2016). It is effective to neutralize traditional road blocks and ambushes. Subsequently, these road blocks are to be organized in a different way, to cope with this new modus operandi.

Some last remarks on the Rumsfeld Matrix. Firstly, it is to be approached as a matrix, and not as a cycle, in the sense that techniques are not applied in a sequential, but in a parallel way. Only the inductive experiments of the unknown-unknown quadrant (Red Team/Red Cell), are to be executed *after* you have carried out your analysis for the other three quadrants. If not, you will infinitely carry out inductive experiments.

Secondly, if you start a new case, e.g. a new PKO, it is likely that your databases are not filled yet. The β gap will now be felt mostly. This may hamper the application of some of the tooling within the unknown-known quadrant, especially the ones that are based on quantitative (abductive) correlations (De Valk, 2018), as in Data Science Cells. As a result, the known-known quadrant then needs an extra emphasis to challenge causal connections made over data. This is needed, among others, because of the persistence of impressions based on already discredited evidence in the causal connection (Heuer, 1981).

Thirdly, for an optimal coverage, it is advised that in the overall matrix techniques are used from all three classes of reasoning – deduction, induction, and abduction (for an explanation, see the next heading). As every class of reasoning has biases and limitations, these are likely minimized by combining them. Only a combination of them

will reduce the number of relationships that otherwise would have been overlooked. Also, to compose the matrix, you do not need to limit yourself to one technique per quadrant.

To summarize, the Rumsfeld Matrix does not only deal with the four different types of unknowns, it also combines both qualitative (EWCI, DBSB) and quantitative aspects (Data Science Cells), and all three classes of reasoning. By this robust methodological approach, it is aimed at not to miss any relevant threat – to reduce the value of the β.

Standard Logic Model: Case-theory and future innovations

After presenting a tool on different combinations of unknowns, we now turn to a tool to assess what part of your case is covered, and to what extent you are prepared for future innovations by other parties in play. It refers to reducing both the α and β. In the tool, the different classes of reasoning – inductive, deductive and abductive – are arranged. This is done in an ordinal way, not an absolute one. However, before we can present the scheme, we first will have to discuss the three classes of reasoning, as they are defined for their effect on reducing the α, but hardly for their effect on reducing the β.

Different classes of reasoning

In the methodological literature, reasoning is defined for their effect on the α. Firstly, in deductive reasoning you argue from the general to the specific – a top-down approach. In a logic way, the conclusions are deductive of the premises presented. An argumentation is deductive, meaning that if the premises are correct, the conclusion therefore will inevitably also be correct. Secondly, there is inductive reasoning – the ex-consequentia reasoning. Here, a general rule – generalization – is made based upon a number of specific observations, experiments etc. These observations and experiments indicate that the premises of an inductive logical argument have some degree of support. It is a bottom-up approach. The conclusions that result from inductive reasoning – and in which the premises are true – *are likely* to be true, but also can be false. Thirdly, there is the inference to the best explanation (IBE), or abductive reasoning, in which an explanation is selected based upon likeliness. In abductive reasoning, it is assumed

that the most likely conclusion is the correct one. It is reasoning through successive approximation (Voulon, 2010).

As formulated above, the reasoning is on how to reach your conclusions and on the absoluteness of your claim (α). However, it is *not* on not to miss relationships (β). To be relevant to the β orientated intelligence research, reasoning needs to be reformulated, and calibrated from an α approach to a β approach. Yet, not only in general literature on methodology, even in intelligence handbooks reasoning is only presented and explained in the context of reducing the α, and not the β (De Groot, 1981; Grabo, 2002; Voulon, 2010). At the Ad de Jonge Centre, University of Amsterdam (UvA), *Red Team* and *Red Cell* experiments were carried out. In such experiments, the unknown-unknown is addressed, to reduce the residual threats. It deviates from the regular scientific experiments in which a hypothesis is tested – and, by that, is related to the α. During these β-related *Red Team* experiments, some insights were obtained on how reasoning may contribute to reduce the chance we miss a threat – i.e. to reduce the value of the β. Without claiming definitive conclusions, the UvA-experiments indicate some strong and weak points for their potential to reduce the value of the β. In a scheme, this can be summarized as follows (De Valk, 2018).

Logic and β?

Hardly developed: some Red Cell experiences

Logic	Strength	Weakness
Deduction	Fast, general inventory + directs research at residual threats.	Weak in making an inventory of a *deviation* from the general pattern. Hardly covers real innovations.
Induction	Maps innovations (new modus operandi). Aims at the unique + Verstehen.	Slow in making an inventory. Maps only a small part of the case (= C-theory).
Abduction	Big data (quantitative): generates many correlations, otherwise overlooked (additional hypotheses) + trends	Often lacks causality (limited relevance of many correlations). Limitations concerning the future (significant amount of data from past & present is needed).

Figure 3: Logic and β? (Source: De Valk, 2018)

Standard Logic Model

As every class of reasoning has biases and limitations, these are likely to be minimized by combining different classes of reasoning in a research. For an optimal reduction of the value of the α, it is therefore assumed that all different classes of reasoning have to be used. Concerning the reduction of the value of the β, the preliminary findings at the Ad de Jonge Centre points the unique weak and strong points for each type of reasoning. It also supports the assumption that it is advisable always to use all classes of reasoning in a threat related case study.

The next scheme is an ordinal presentation and not an absolute one. The reason is that it is work in progress, and not a fully developed model. It has been composed after testing and reflection of intelligence analysts on how logic contributes to a case-study. This is done for two aspects: firstly, to compose a C-theory (x-axis); and, secondly, to be prepared for future innovations by the parties involved (y-axis).

The three forms of logic are represented by a color: abductive (yellow), inductive (red), deductive (blue). Abductive reasoning (yellow) will be for a large part composed of finding quantitative correlations, as, for example, by Data Science Cells. To find a correlation, things must already have happened to some extent in the past. So, future innovations can be assessed, but only limited. That is why they are positioned at the bottom half. On the other hand, these big data will result in a large number of correlations, and therefore it covers a large area of the case.

In inductive reasoning (red) – by 'Verstehen' (Weber) as in, for example, Red Team – elements are less connected to the overall picture – the C-theory. That is why they are put on the left side. But they can prepare you for future innovations, even an opponent had not thought of yet. That is why they are listed at the top of the y-axis.

Finally, in deductive reasoning, inventories are made, for example, on possible futures. Afterwards, scenarios and indicators are composed to monitor what scenario eventually will be the most likely one. It covers all main likely futures and makes an inventory of the elements in play. It both contributes to the C-theory building and assessing future developments. Therefore, it is positioned right-top. It results in the next ordinal – not absolute – areas in the following scheme.

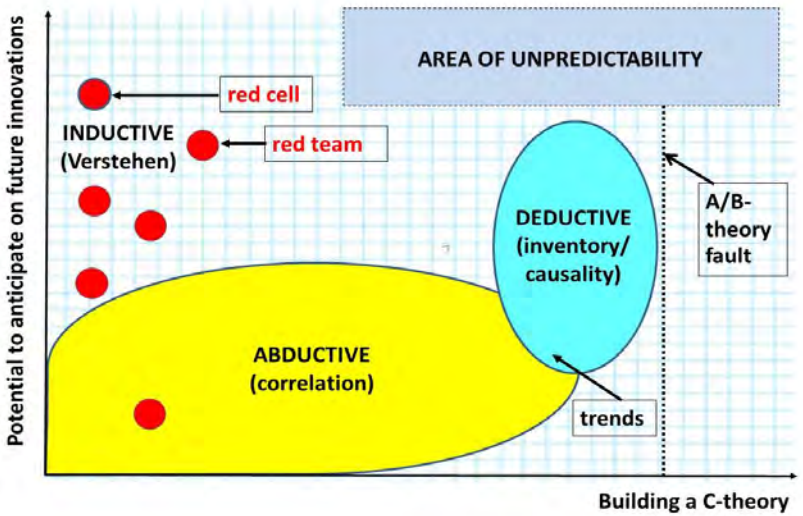


Figure 4: C-theory building (author's approach)

A methodological disclaimer needs to be made. In methodology, logic is mainly developed to apply A/B- theory to a case, less for logic *within* a C-theory, and not at all for the β. Right of the A/B-theory fault, the traditional α oriented insight of reasoning and logic is in place. The whole field left of this fault is nothing more than an ordinal representation. Yet, the relevance of the scheme is that we now can assess what we have covered of our case already, and where most likely our white spots are. Still, there will always remain an area of unpredictability (top-right).

The Standard Logic Model encompasses three elements. Firstly, it includes both the α and β aspects concerning the way correlations and causalities found (α), and of what you may have missed in the overall picture (β). Secondly, all three logic forms of logic are included. And finally, it encompasses both the qualitative and quantitative aspects of a research. All are represented in one overall scheme. In the next section, we will deal with a sub-optimal approach, and how you can develop it into a more optimal one. As put, this illustration will be on a PKO mission.

Standard Logic Model: SAT's and tooling

This section will start with a sub-optimal situation of an analysis. It will be illustrated how a more optimal situation can be reached. Actual methods will be presented.

A sub-optimal way of using logic in a case.

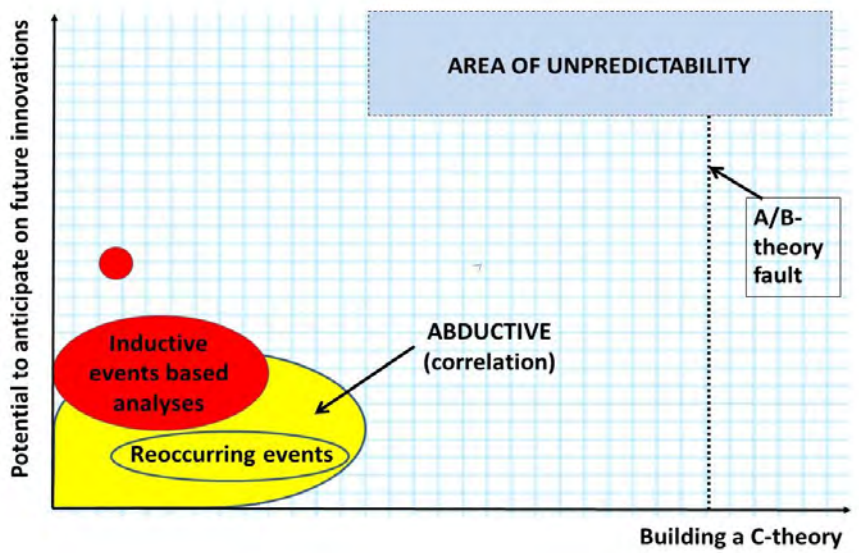


Figure 5: *A sub-optimal way of using logic in a case*
(author's approach)

To what failures could this lead to? A simple illustration. Say, there is a new type of youth gang. After a certain time, the street violence diminishes, and the police make an inductive event based analysis only (scheme above). It concludes that there is less violence, so society has a lesser problem now. If a Driver Based Scenario Building had been carried out, it may have resulted in an opposite outcome. What were the drivers behind this 'appeasement', because not only the chapter in the capital, but *all* the chapters of this gang, including in the border area and the small harbors, suddenly committed no street

violence anymore? The main driver was that the gang became big in the international drug trade and did not want any unnecessary attention. The gang changed from petty crime to undermining or disruptive crime. As such, this calls for more police investigation instead of less, but it remains unveiled if you limit yourself to an event based analysis instead of a driver based one.

If you make, in a PKO, an inductive event based analysis, you will miss the deeper drivers of developments. It is exactly these drivers that yield the mid- and long-term insights. So, the policy planning will be hampered and the PKO will be less prepared on the mid- and long-term. But also, the potential of near term warning will be limited. Grabo's ground breaking research on failures of sub-optimal analysis led to the development of an elaborate early warning and critical indicator approach (EAPC, 2001). Furthermore, computer systems need to be filled with data to provide automated alerting on those critical indicators. Finally, as Red Team/Red Cell is absent, the analytical unit will be unable to reflect accurately on possible new modus operandi by the other parties. Thus, it cannot be anticipated on them. In the next sub-section, it will be – step by step – explained how this gap can be filled by SAT's and tooling, so that a case-theory can be build that includes future developments also.

(Sets of) techniques and Structured Analytic Techniques (SAT's)

How can you transform the presented suboptimal situation, into a more optimal one? The presented approach is based on inductive events analysis. Furthermore, this PKO makes scenarios for reoccurring events, as, for example, annual clashes between farmers and cattle keepers (scheme above). Yet, no elaborate scenarios should be building, but these events should be mitigated for their impact only. Scenario building in case of reoccurring events is a waste of energy and resources of the analyzing unit. How could you improve the presented situation? The following suggestions are meant as an illustration only, to show how the Standard Logic Model can be a steering instrument for, for example, the planning of your training and education. For an elaborate explanation of most of the following techniques, see Heuer/Pherson, 2011.

A first set of techniques is needed for your policy planning on the mid- and long-term. You want to know in what different ways the situation may develop, and then formulate for each of those options a policy to cope with it, so you are prepared to act if it occurs. A set of techniques could be a Driver Based Scenario Building approach. It is composed of two columns. The left column is to generate hypotheses and to test them for the data (events) available. The right column is to analyze on a deeper level the drivers that drive the events and pattern of events. This can be done, for example, by assessing the drivers on actors through a Strength Weakness Opportunity and Threat (SWOT) analysis, and assessing the drivers on factors through a Causal Loop Diagram. Subsequently, the drivers with the highest impact and highest uncertainty are selected as the axes that are the basis to build the scenarios on – together with wild cards and trends. Finally, all these scenarios will be the input for the hypotheses (x-axis) of Analysis of Competing Hypotheses (ACH), and the data of the event column will be the input of the evidence (y-axis) of ACH. Thus, the factual observed events are tested against the deeper level of analysis (drivers), and vice versa. It has the potential to reveal yet undisclosed deception within the realm of the events (the 'evidence' of ACH), and vice versa. This way of scenario building was experimented with in 2018 in the Minor Intelligence Studies at ISGA, University of Leiden.

This approach results in an inventory of all main courses of action possible (β), but also assesses what the most likely ones are, including by assessing the speed and direction in which drivers will develop (α). In the techniques, all classes of logic are used at some point of the process. As you cover all the main options, you are working on your C-theory. As it is on the mid- and long-term, it will be somewhere middle/top. Therefore, this set of techniques will be situated somewhere at the right-middle/top of the Standard Logic Model.

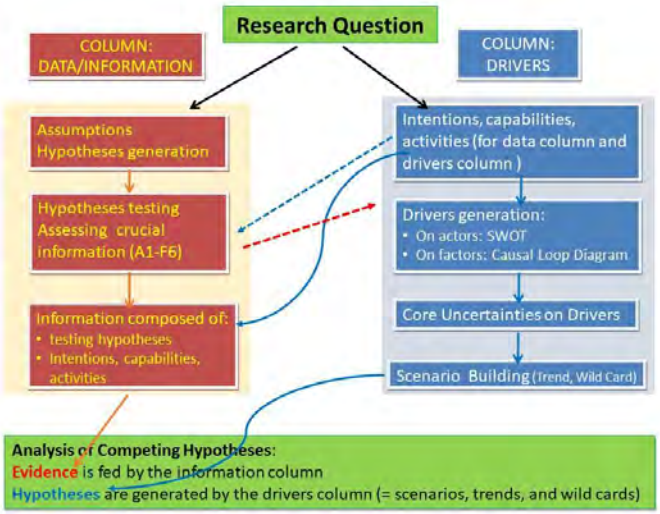


Figure 6: Standard Logic Model (author's approach)

Secondly, besides a policy planning on the mid- and long-term, you also want to act on the near term when a threat actually occurs. If possible as early as possible. Based on the work of Grabo (Grabo, 2004), a set of techniques has been developed to warn as early as possible by monitoring so-called critical indicators (EAPC, 2001). Such a research starts with formulation of a *Warning Problem*. Then *Warning Scenarios* are developed for the possible outcomes of this specific *Warning Problem*. For each scenario, a set of *Critical Indicators* is developed that is unique for that specific scenario only. Finally, an *Intelligence Collection Plan* is made to monitor the development of these indicators. When an indicator changes from normal (green) to, for example, an extreme state (red), the analyst decides if a warning is needed. The warning process needs to be supported by good data management and preferably by an automated alerting on the *Critical Indicators* if the status of an indicator changes.

It results in an inventory of the scenarios to warn for on the near term. All main scenarios to warn for are covered (β), and the Critical Indicators tell if a specific scenario actually will occur (α). As it is on the more specific warning issue, it will contribute less to the C-theory than

Driver Based Scenario Building (middle-right). It is also on the near term, instead of on the mid- and long-term, therefore it is situated around the middle of the y-axis. So, this set of techniques will be situated somewhere at the middle-right of the Standard Logic Model.

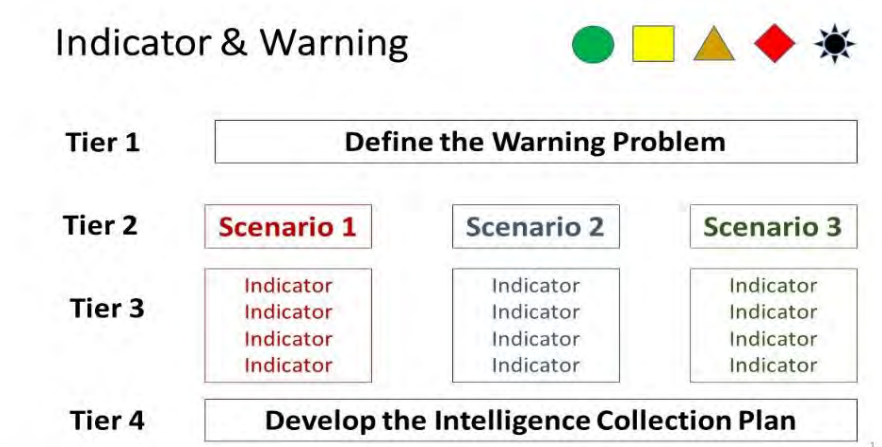


Figure 7: Driver Based Scenario Building (author's approach)

A third set of techniques is Red Team/Red Cell. It is an experiment in which – through inductive reasoning ('Verstehen') – it is assessed, for example, what new modus operandi may be developed by another party that has not been used yet. It deals with the unknown-unknown (β). These experiments are hardly connected to the overall picture – the C-theory. Therefore they are situated at the left. But they can prepare you for future innovations, even this other party itself has not thought of them yet. That is why they are listed at the top of the y-axis. As they are relatively isolated experiments, they will only cover a small part of the total picture (red dots).

A fourth group deals with the quantitative approach. We live in a time of information overflow and need to process enormous amount of data that can never be processed in that quantity by humans. Furthermore, often real time intelligence is needed (by machines), instead of close to real time (by analysts). Machine Analysis plays a

central role here. It can be organized in a so-called Data Science Cell. Different aspects of Machine Analysis can take place, as shown in the scheme below. In the scheme RGAP stands for Research Guided Action Planning. The way machines reason, learn, and analyze, is presented in the next scheme (De Valk, 2019a).

Machine learning will be often based on a more abductive way of reasoning. It will yield enormous amount of correlation (large area of coverage, α). Correlations that would not have been included if only humans were looking for them (β). The results are not always connected to the C-theory (from left to right). As the data must be in the system – have taken place in a significant manner – the future orientation will be limited (bottom-to middle), although it will, for example, generate a lot of trends. That is why it is situated as the big yellow area at the lower half of the model.

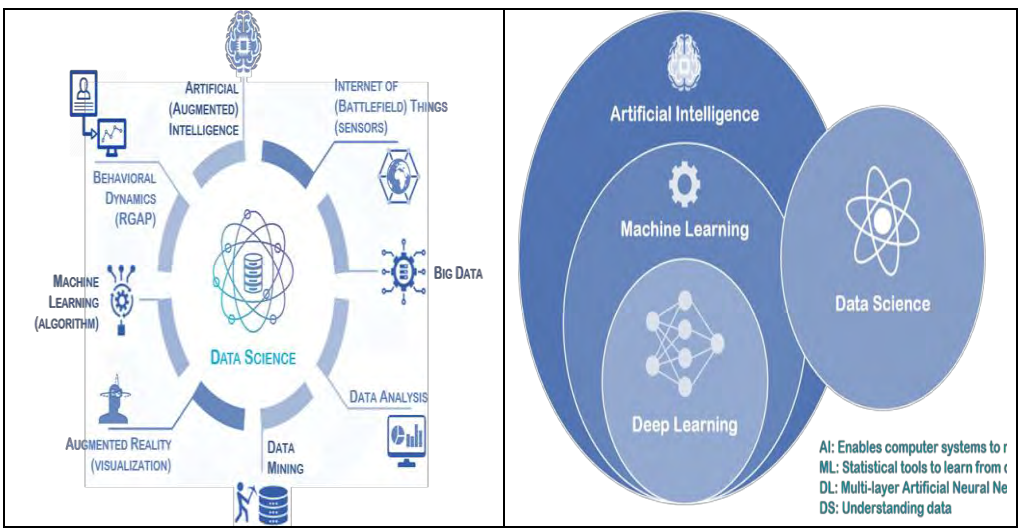


Figure 8: The way machines reason, learn, and analyze
(Source: De Valk, 2019a)

If we put all the techniques and tooling in place, it will result in the next scheme. The different element will support each other. A Data Science Cell, including the input from criminal profiling, geographic

profiling, spatial analysis, social network analysis, SOCMINT and GEOINT, will be used, for example, to compose, to refine, and to assess the scenarios. It will also lead to a better source management by a more optimal assessment of the reliability of the source (A-F), and the credibility of the information (1-6) (*AJP 2.0*, 2002).

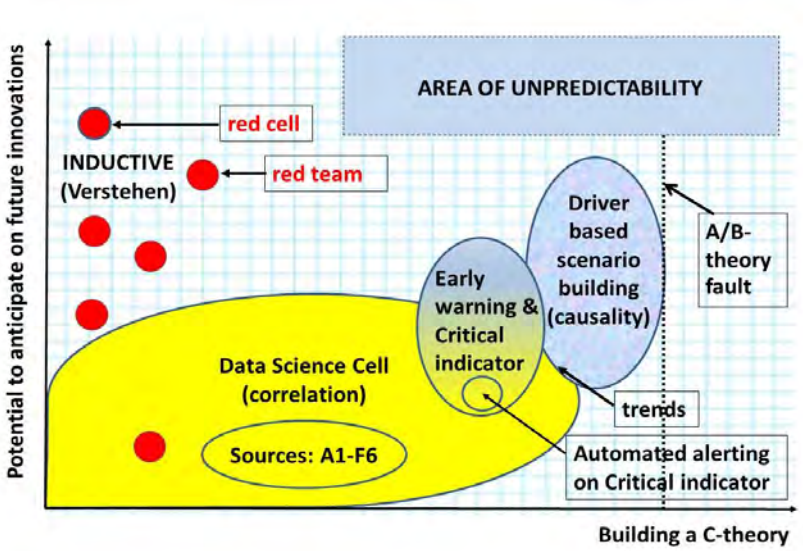


Figure 9: C-theory building (author's approach)

The aim was to illustrate, how the Standard Logic Model can help both to plan (what you need) and to evaluate (what you may have missed) your intelligence process. It can be used as a planning instrument for your training and education program. It also indicates that the combination of human and machine analysis will result in a more genuine threat intelligence (Pace, 2018). This way, it can contribute to the so-called Augmented Intelligence in which humans and machines are paired in their analytic effort (Sabhikhi, 2017).

The incomplete practice – the case of positive vetting

Another illustration would be if we are confronted with a situation in which you never will reach an optimal combination of

techniques – as in the PKO example – because the files are not kept, the options are too divers, and the incidents too unique to formulate scenarios for. Can the Standard Logic Model still provide insight to evolve to a more optimal situation? An illustration is presented for positive vetting. HRM officials do not like disclosure on this sensitive issue, so data are presented in an anonymous and abstract way.

Let's assume, we have the next system of positive vetting in place. Firstly, it is assessed if the candidate does not pose a risk by its personality or by being potentially subject of black mail. Secondly, it is assessed if the candidate is not part of a vulnerable environment. Apart from extensive file checks, it is also composed of an extended interview of several hours by two persons – one to interview, and one to observe. In the whole vetting process it is tried to assess that the candidate cannot be black mailed (alcohol, drugs, sex, money, past, etc.), and hasn't had an extremist or violent history. The emphasis is on information of 16+ years of the candidate. Also, it is tried to assess that there are no vulnerabilities in the environment of the candidate, as extremists, criminals, or visits of and influencing by suspect countries. The approach is to assess. To asses implies it is mainly an α oriented approach.

What is the problem in this setting? HRM officials do not like disclosure, so colleagues cannot learn from incidents. Furthermore, a different culture is needed, especially at the HRM office. Often, HRM steers on mistakes, and is not a safety net for people that have (personal) problems. The effect is that the person in question, in case he/she is vulnerable (e.g. a life changing event), will not contact HRM for help. Colleagues will hardly have incentives to report on suspect indicators. And superiors hardly will keep files. This applies to many Dutch organizations. It results in a too little & too late situation (Houtzager, 2018).

A complicating factor is that there is no typical profile of someone taking the wrong turn. Actually, in reconstructions, about 75% had no problems when he/she accepted the job. There are some weak correlations – having an open ended contract, working more than 10 years at the same organization, experiencing a life changing event, and having a Narcissistic personality are overrepresented. But the

correlations are far too weak to compose scenarios for in which indicators are developed that will be monitored. The picture of offenders is too divers (De Valk, 2019b).

As data are simply absent, it is hard to rely on big data correlations. So the yellow field of quantitative abductive correlations will be limited, even close to absent (yellow: bottom half). Offenders and incidents being too unique will make it hard to compose scenarios for (blue-red: middle-top, right). As a result, it is hard to develop a system of critical indicators, even more so as colleagues hardly have incentives to report, and superiors hardly will keep files (blue-yellow: middle, right). It ends up as the following situation for the Standard Logic Model:

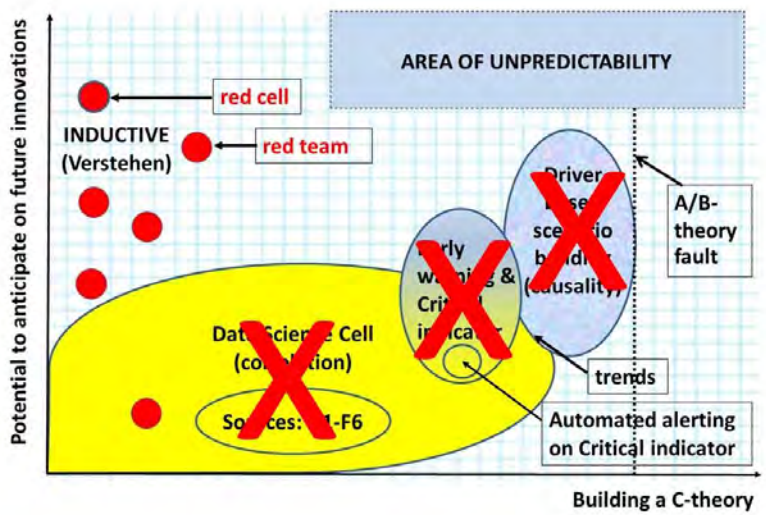


Figure 10: C-theory building (author's approach)

What is left in the original scheme are the red dots at the left. It is on experiments on eventual undisclosed weaknesses. If that was to be included into the vetting process, it would result in an on-the-job testing of the integrity of an employee. The vetting system would then shift from a pre-employment into an in-employment or during-

employment approach. It would lead to some adaptions compared to the original approach. The employee can now be tested on its vulnerabilities. It could be represented as three phased strategy to *deny* that the candidate is a *threat*. It starts with a long interview, preferably by one person to build up report. The interviewer will ask the candidate to describe him/herself nowadays, and then go back in time, finally with also a focus on 3-7 years old – to assess more primal reaction patterns of the candidate. Then they, together, assess the candidate's vulnerabilities, and develop a plan to cope with these vulnerabilities. Finally, the candidate will be tested – Red Teamed – during his/her entire career on these vulnerabilities. The approach will shift from an α (to assess) into a β (to test in order to deny that there is a threat) approach.

The second illustration indicates that the Standard Logic Model can provide a methodological underpinned improvement for an imperfect situation as well. Knowing this, the Standard Logic Model could also be used the other way round. For example, in a state on state situation, an opponent does not employ elaborate 'Verstehen' experiments (Red Teams, wolf packs with a free role to monitor the movements of an opponent etc.) for its defensive counterintelligence. You then only have to analyze its counterintelligence SOP's to create your red carpet into that country. The Standard Logic Model can serve different functions – how to design your analysis in an optimal situation (PKO), how to improve it in an imperfect situation (positive vetting), and how to analyze weaknesses to attack the opponent (counterintelligence).

Reasoning and the Rumsfeld Matrix

After the illustrations of the Standard Logic Model, we now return to the Rumsfeld Matrix. Some quadrants of the Rumsfeld Matrix seems to prefer certain classes of reasoning, although other classes of reasoning are not excluded completely. The unknown-unknown quadrant will almost exclusively rely on inductive reasoning, since Red Team/Red Cell has a 'Verstehen' approach, and takes place in the setting of a β *experiment* (De Valk, 2012). The unknown-known quadrant will be dominated by abductive reasoning (big data), but

inductive reasoning will be present, as in statistical syllogism (a syllogism – Greek for conclusion or inference – is a logical argument in which a conclusion is based on two or more propositions that are asserted or assumed to be true; unlike many other forms of syllogism, a statistical syllogism is inductive). In the known-known quadrant, abductive reasoning will play a main role in belief revision – to take into account a new piece of information. In the known-unknown quadrant, all three types may be present. The type of logic largely depends on the technique chosen. Deductive techniques of this quadrant will be of help to get fast, general, inventory, in order to look for the residual threats to be addressed.

The difference between the Rumsfeld Matrix and the Standard Logic Model is that in the Rumsfeld Matrix the different types of *unknown* are addressed by selecting analytical *techniques*. In the Standard Logic Model, it is shown how the different *classes of logic* interact, and how they, together, *compose* the future oriented *C-theory*. The two tools – the Rumsfeld Matrix and the Standard Logic Model – are complementary in designing a threat related, future oriented, C-theory.

Conclusion

Intelligence analysis takes place in a context of deception and denial, in which opponents constantly innovate themselves. In that context, you don't want to miss threats. A research design tool is needed to cope with the unknown, or, in methodological terms, to reduce the value of the β. The presented tool, the Rumsfeld Matrix, can help to identify different types of unknowns in which data or technique/tooling is missing. In this Rumsfeld Matrix, both the quantitative and qualitative approach is integrated. Also, all three types of logic can be applied. Thus, the change of missing relevant relationships on threats is reduced.

Next, the Standard Logic Model assesses to what extent a case study has been covered in terms of logic. Abduction, as it is implemented now in quantitative analysis, is good at producing large quantities of correlations. Deduction is strong at making inventories, and induction is good at anticipating on new innovations by an opponent.

With the help of the Standard Logic Model it can be visualized what the current overage of a case is, and what the desired state would be. It assesses what sets of techniques will cover what aspects. For the long term, Driver Based Scenario Building deals with both case-theory building and future developments, and is suited for policy planning. Early Warning & Critical Indicator does the same on the near term, and is oriented at acting on threats. Red Team and Red Cell experiments are good to anticipate on possible innovations by an opponent, as new modus operandi. Finally, the establishment of Data Cells will result in quantitative and automated calculation and processing of data, and even in analysis. The model assesses where additional training and education is needed, or additional Data Cells need to be implemented. If an optimal situation cannot be reached – it can be assessed what alternative solutions are possible, as was the case in the illustration on positive vetting.

The Standard Logic Model integrates three aspects. Firstly, all three forms of logic, abduction, deduction, and induction, are included. Secondly, it combines both the qualitative and quantitative approach. Thirdly, analysis by humans and analysis by machines can be combined. It will lead to an enhanced way of working – that of augmented analysis in which machines and humans are paired in their analytic effort.

Where the Rumsfeld Matrix is a tool specialized to design a β oriented research, the more general Standard Logic Model is both suited for an overall planning of the analytic needs, as well as an instrument to evaluate. The combination of the Rumsfeld Matrix and the Standard Logic Model can be used to refine the process of preparation, composition, and evaluation of threat related intelligence case research. The Rumsfeld Matrix can, per quadrant, fine-tune what specific techniques and/or data are needed not to miss a threat. In combination with the Standard Logic Model, it is – in an ordinal way – visualized what part of the case-theory has been covered, and to what extent it has been anticipated on future developments and future innovations.

References:

1. *AJP 2.0. Allied Joint Doctrine for Intelligence, Counterintelligence and Security.* NATO, 2002.

2. De Groot, A.D., (1994), *Methodologie: Grondslagen Van Onderzoek En Denken in De Gedragswetenschappen*. Assen: Van Gorcum.

3. De Valk, Giliam, (2011), "Effectiviteit vanuit methodologisch perspectief: welke gevolgen heeft de introductie van nieuwe methoden en technieken?" In *Contraterrorisme en ethiek*, edited by Michael Kowalski and Martijn Meeder, 69-82. Amsterdam: Boom.

4. De Valk, Giliam, (2012), "Red Team and Science." Presentation at De Nederlandsche Bank (DNB), Den Haag, June 8.

5. De Valk, Giliam, and Willemijn Aerdts, (2018), "Inlichtingenwerk Vanuit Een Methodologisch Perspectief." *Justitiële Verkenningen* 44, no. 1, pp. 114-32.

6. De Valk, Giliam, (2019), *Analytic Blackholes*. Unpublished Paper. Dutch Ministry of Defense.

7. De Valk, Giliam, (2019), "Critical Infrastructure and the Insider Threat." Presentation at The Zagreb Security Forum, Zagreb, March 15.

8. *DoD News Briefing - Secretary Rumsfeld and Gen. Myers*, (2002), United States Department of Defence. February 12, retrieved from https://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636.

9. *Generic Early Warning Handbook*, (2001), Report. EAPC/Council Operations and Exercise Committee. NATO.

10. Goldbach, Onno. Letter to the author, 2012.

11. Grabo, Cynthia, (2004), *Anticipating Surprise: Analysis for Strategic Warning*. Lanham: University Press of America.

12. Heuer, Richard, (1981), "Biases in Evaluation of Evidence." *Studies in Intelligence*, winter, pp. 31-46.

13. Heuer, Richard J., (1999), *Psychology of Intelligence Analysis*. Langley: Centre for the Study of Intelligence, CIA.

14. Heuer, Richard and Randolph Pherson, (2011), *Structured Analytic Techniques for Intelligence Analysis*. Washington, DC: CQ Press.

15. Houtzager, Wil. Lecture at University of Leiden, 11 October 2018.

16. Menkveld, Christiaan. Lecture for '*de Leergang*' at ISGA, University of Leiden, 2018.

17. Moore, David T., (2011), *Sensemaking: A Structure for an Intelligence Revolution*. Clift Series on the Intelligence Profession. Washington, DC: National Defense Intelligence College Press, retrieved from http://ni-u.edu/ni_press/pdf/Sensemaking.pdf.

18. Pace, Chris, ed. (2018), *The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence*. Annapolis: CyberEdge.

19. Sabhikhi, Akshay, (2017), *Augmented Intelligence. Executive Guide to AI.* Austin, Texas: Cognitive Scale, retrieved fromhttps://www.cognitivescale.com/wp-content/uploads/2017/05/Augmented_Intelligence_eBook.pdf.

20. Silver, Nate, (2012), *The Signal and the Noise: The Art and Science of Prediction*. London: Allen Lane.

21. Treverton, Gregory F., (2009), *Intelligence for an Age of Terror*. Cambridge: Cambridge University Press.

22. *The Red Team Handbook.* (April 2012), Report. University of Foreign Military and Cultural Studies, retrieved from https://usacac.army.mil/sites/default/files/documents/ufmcs/The_Red_Team_Handbook.pdf.

23. United States. Department of the Army. FM 34-2 Collection Management and Synchronization Planning. March 1994, retrieved from https://www.globalsecurity.org/intell/library/policy/army/fm/34-2/index.html.

24. *Urban Operations III: Patrolling.* Student Handout. Marine Corps Training Command, retrieved from https://www.trngcmd.marines.mil/Portals/207/Docs/TBS/B4R5579XQ-DM Urban Operations III – Patrolling.pdf?ver=2016-02-10-114414-840.

25. Van Strien, P. J., (1986), *Praktijk Als Wetenschap: Methodologie Van Het Sociaal-wetenschappelijk Handelen*. Assen: Van Gorcum.

26. Voulon, Rosa, (2009), *Handboek Analyse. Theorievorming En Methodologie in Inlichtingenanalyse*. 't Harde: Defensie Inlichtingen En Veiligheids Instituut.

27. Yin, Robert K., (2014), *Case Study Research: Design and Methods*. Los Angeles: Sage.

ECONOMIC INTELLIGENCE AND NATIONAL SECURITY: TOWARDS THE DEVELOPMENT OF THE COOPERATION BETWEEN THE BUSINESS COMMUNITY AND THE PUBLIC SECTOR

Răzvan GRIGORESCU*

Abstract

In this paper, we will analyse the opportunity of developing a cooperation between the business community and the public sector, from an economic intelligence perspective, aiming to improve the economic security of Romania. The research question we try to answer is "How can Romanian companies and the national intelligence services cooperate, in order to improve our economic security"?

Taking into consideration the various threats to the economic security of our country, in this paper we choose to briefly analyse the existing relationships between competitive and economic intelligence, as well as the concrete ways in which private companies and public intelligence services can cooperate, in order to counter the economic and/or industrial espionage. We believe that our approach can pave the way for further research that will contribute to the formulation of useful recommendations, for both Romanian companies and the public sector.

Keywords: *economic security, economic and competitive intelligence, economic and industrial espionage*, *business community.*

Introduction

In our attempt to find new ways of improving the national security of Romania, in this paper we will analyse the opportunity of developing a cooperation between the business community and the public sector, from an economic intelligence perspective. The research question we try to answer is *"How can Romanian companies and the national intelligence services cooperate, in order to improve our economic security?*" In order to answer the research question, we are going to use

* PhD Candidate, "Mihai Viteazul" National Intelligence Academy, Romania.

various open sources to collect and analyse relevant information on how the performances of the business community influence the economic security, as well as information on the possible dimensions of a cooperation between the private owned companies and the governmental institutions, considering the existing international security environment and the possibility of using the competitive intelligence function for national security purposes.

We estimate that some of the conclusions drawn from this work would be used for further research, having the capacity to contribute to the formulation of useful recommendations, for both the Romanian business community and the public sector.

Economic security and business performing

During the first half of the 20th century, Constantin G. Demetrescu noted that "the means by which a nation is enriched is the profit achieved by each enterprise" (Demetrescu, n.d., p. 7). At the same time, he emphasized that "the enterprises, through their profitability, as well as through the incomes of their employees, contribute to the securing of the state's revenue to cover public expenditures" (Demetrescu, n.d., p. 6), and "through their relations in other States, to the economic and political life of a nation" (Demetrescu, n.d., pp. 6-7).

Nowadays, the Romanian business sector is confronting a tremendous international competition. Theoretically, competition has a positive impact to any business, being an important motivational factor in terms of stimulating creativity, innovation and productivity.

Nevertheless, sometimes, competition is influencing the economic performances of the companies negatively, due to the missing expertise in handling it properly. In the current international business context, competitors can be located in any of the key markets of the private companies. Very often, these competitors are interested in maximizing their market shares and their profit margins, fast. For this purpose, some of them might sometimes resort to practices that are at the limit of legality or even illegal. These competitors might originate in friendly/allied countries or in countries with which we do not share common values.

Based on the Romanian Intelligence Service approach that "A performing, competitive and stable economy is a vital pillar of national security" (Serviciul Român de Informaţii, n.d., Economic Security, para. 1), we observe that given the existence of a free market economy, in which private capital prevails, the economic performances of the private owned companies directly influence the national economy and national security. In some cases, non-state entities become so strong that they compete with the state ones. Up to now, six main types of non-state actors have been distinguished: private corporations, NGOs, international organizations, regional organizations, virtual organizations, criminal cartels and terrorist organizations (Sava, 2005, p. 140). Presently, one of the most common business threats coming from non-state entities is represented by the industrial espionage. More than that, it should be noted that sometimes non-state entities might benefit from the support of state entities, being involved in illegal activities of economic espionage.

Analysing whether economic espionage is a topical issue that should concern us, or not, we concluded that it represents a real threat that should concern us, as it has the potential to cause serious harm to our national security. Practically, we can estimate that being a member state of the European Union, a member state of NATO and having an excellent Strategic Partnership with the United States of America, our country is becoming a very attractive target of espionage, for different non-state and/or state entities, such as the Russian Federation.

Since the early 1990s, German intelligence services reported that a number of Russian intelligence officers "left" secret services become engaged in German or Russian companies without breaking their ties with their former employers (Whitney, 1993). We would like to emphasize that after the end of the Cold War, the "economic espionage has been globalized" (Petrescu, 2011, p. 259) and a new war began, the economic war, with a strong informational component (Petrescu, 2011, p. 282), in which state and various non-state entities are involved.

Referring to the attitude of countries to engage in economic espionage on political and/or military allies, one of France's former directors of DGSE, Pierre Marion said that although France is a military

or political ally with different states, "in the economic competition, in the technological competition we are competitors; we are not allied." ("Economic Espionage", 1992) Analysing the different implications of the economic results of the private companies in relation to our economic security, we focused on the best possible ways in which the Romanian companies can cope with their competitive business environment, of which we chose the one related to the use of the expertise of the intelligence community, following the similar examples of other countries.

Taking into account this diversification of the non-state entities that also have the potential to influence the economic security, we believe that the private companies should study the possibility of cooperating with the governmental institutions in different ways, being able to effectively support each other, for the wellbeing of the nation. It is well known that from a national security perspective, the economic dimension decisively influences other dimensions of security, including its military one. As far as economic intelligence is concerned, it is linked to commercial, monetary, agricultural or industrial policies, as well as to the economic practices of a country as a whole. (Nedelea, 2014, p. 132)

Noting the need of developing the private intelligence sector, Bonnie Hohhof highlighted that government intelligence can significantly support competitive intelligence in private organizations, actively sharing new intelligence developments, underlining that more can be done (Hohhof, 2014).

Following this idea, we observed that in Canada, being aware that the international business environment has become more competitive year after year, the Canadian government tried to identify and develop the possible roles it could have in competitive intelligence, in order to help Canadian companies perform better. Following this approach, five main roles of the government were identified, including the role of partner (e.g. joint CI programs to industrial and training groups in the CI – perhaps the most important role) and of mentor (former intelligence officers help companies to implement CI functions). (Calof, 1999, pp. 20-23) At the same time, in Germany, BfV has entered into cooperation agreements with different industrial players, such as

the Federal Association of Security Companies and the Federal Union for IT, Telecommunications and New Media, in order to improve the protection of the know-how and informing companies about the risks of espionage. (Agheană, 2017)

Cooperating for national security

In this paper, we choose to briefly analyse the existing relationships between competitive and economic intelligence, as well as the concrete ways in which private companies and the governmental intelligence services can cooperate, in order to counter the economic and/or industrial espionage. We consider important finding new possible ways in which the threat of espionage could be addressed, as it is a known fact that it could bring serious damages to states economies, its targets being both from governmental and non-governmental area.

In the National Security Strategy (2017), the first during Donald J. Trump's Administration, the importance of protecting US intellectual property against the theft of information by various competitors it is mentioned, making an explicit reference to China, which would steal annually intellectual property of hundreds of billions of dollars. ("National Security Strategy", 2017) Gerald P. Burke mentioned more than two decades ago that the Chinese use some visiting delegates in developed countries to conduct economic espionage, and that some Chinese companies are frequently involved in various industrial espionage activities. (Burke, 1992)

In connection with the illegal actions carried out by some Chinese citizens in Romania, with the potential to affect the national security of our country, we would like to highlight the example of Wang Yan, a Romanian citizen of Chinese origin, to whom the Romanian citizenship was withdrawn, on the recommendation of Romanian Intelligence Service, as his actions would have harmed the national security. (Neag, 2018)

At the same time, we would like to recall the case of IPROMIN SA, were investigated by DIICOT from 2012, which came to the attention of the general public in regard with the "illegal collection of information, including classified ones", that had the potential to affect the economic security of Romania. A Russian citizen carrying classified documents

was detected by the Counter-Terrorism Brigade specialists of the Romanian Intelligence Service, following a routine check on the Henri Coandă Airport. (Olescu, 2012)

The economic espionage can be mainly detected and neutralized through specific activities carried out by the state institutions, such as the Romanian Intelligence Service which is "committed to identifying, preventing and countering espionage activities carried out by foreign intelligence services in our country against the interest of Romania and its allies" (Serviciul Român de Informaţii, n.d., Counter-espionage, para. 1). However, even if the expertise, efficacy and professionalism of the Romanian Intelligence Service are unquestionable, given the significant number of the aforementioned non-state actors that could be involved in such activities, we consider that the private companies could develop a transparent cooperation with the Romanian Intelligence Service and other governmental institutions, through their competitive intelligence functions, for economic security purposes. In this respect, some necessary measures must be taken, of which we would like to mention: regulating the unclassified knowledge transfer from the national intelligence services to the business environment (e.g. for trainings, for offering support in the competitive intelligence function development etc.), setting up specialized counterintelligence bodies, which could represent a bridge between the public and the private sectors, as well as the developing of different new academic programs, following the example of the United States of America where various university training programs on the protection of trade secrets and economic counter-espionage are in progress. (Petrescu, 2011, p. 274)

Analysing the evolution of globalization on its economic dimension, Iulian Fota points out that the state will be forced to look for new ways to protect the economic security, against the risk of losing the real control over its economy. (Fota, 2013, p. 95) Taking all these aspects into account, we would like to make some references to the competitive intelligence function, briefly highlighting what it does and how it can be used in national security purposes. It should be mentioned that in our approach, competitive intelligence is directly related to economic intelligence. In our understanding, the competitive intelligence function has a proven value in most enterprises, in terms of

their economic performances, in two main directions, offensive and defensive.

The offensive component of the competitive intelligence function aims at gaining competitor intelligence, market intelligence, strategic intelligence, technological intelligence or social media intelligence, in order to improve the decision-making process and obtain a competitive advantage, clearly mentioning that it only involves the ethical and legal collection of information, having no connection with espionage (competitive intelligence is a legal activity; spying is illegal). Being focused on helping the decision-makers to take the best business decisions and gain a competitive advantage, the competitive intelligence function could be also useful in achieving national security, on its different dimensions, including its economic one (if we choose to consider the interdependence between the economic performances of the private companies and the Gross Domestic Product, for example). To exemplify, through competitor intelligence a company could find out that a particular competitor is "employing" illegal migrants, that represent potential useful information for the governmental intelligence agencies, at least from a counter-terrorist perspective, as it is well known that amongst illegal immigrants terrorists could sometimes infiltrate. In the same time, companies that practice illegal logging or buy wood material about which they know that it has been illegally cut can be identified, illegal logging representing a real threat to the national security of Romania.

The defensive component of the competitive intelligence (mainly aiming to counter competitive intelligence and to preserve the competitive advantage and the differentiation capacity/potential of the company) is primarily targeted at identifying and eliminating company's vulnerabilities that can be exploited by different entities that aim to obtain information from the company, legally or illegally (e.g. strategies, pricing policies, technical features of future products etc.). By using defensive competitive intelligence, private companies are able to take the proper ethical and legal measures which allow them to be more secure, being also in the position to identify trade secret thieves, cyber criminals, or industrial and economic spies.

Practically, through the cooperation between the national intelligence agencies and the privates owned companies, via the competitive intelligence function, national security is winning. We consider important to mention that, in our approach, this cooperation is mainly intended to be carried out in order to ensure domestic security and should not be related with foreign intelligence.

Concerning the legality and ethics of competitive intelligence, we consider that the competitive intelligence functions within the private owned companies should not be required to have legal obligations in the field of national security, regarding information provision, these being mainly focused on generating a competitive advantage to the companies, as a business practice. However, as a proof of Corporate Social Responsibility, we consider that, in some very specific cases, reasonable suspicions could be signalled to the competent national authorities in the sphere of national security. In our approach, these suspicions should be transmitted in a formal manner, together with the transparent mention of the key elements that formed the basis of the suspicions, including the sources that have been used to collect the relevant information (thus being identified or prevented various possible abuses, unfair competition attempts etc.).

Achieving National Security in the New Millennium

At the beginning of the new millennium, the international security environment faces various challenges. Taking into account the risks to which citizens may be exposed, the actual Director of the Romanian Intelligence Service, Eduard Hellvig, emphasizes that at present "the citizen no longer has the classic role of security consumer, but can and must become an active participant in achieving security" (Serviciul Român de Informații, n.d., Security strategy, paragraph 2). In the same time, the linking between this institution and the Romanian society have the potential to lead to the achievement of an extended security. (Serviciul Român de Informații, n.d., Security strategy, para. 2)

Appealing to the memory of recent years, we must emphasize that the idea of involving citizens in national security is not a new one, the Romanian Intelligence Service having this kind of initiatives also in the past, a proof in this respect being the opening that the "Mihai

Viteazul" National Intelligence Academy had in relation to the civil society, by organizing different educational programs, such as Master programs and PhD studies, by cooperating with other Romanian universities, by being present on social media and editing different periodical publications (*Intelligence* and *Romanian Intelligence Studies Review*) etc. Robert David Steele has shown already that for every nation, the informational continuum encompasses several sectors of society, such as schools, universities, libraries, business community, private detectives and information brokers, the media, government, defence, and the intelligence community. Considering the actual international context, in the idea of redefining government intelligence, Robert David Steele believes that for the sake of society, it is necessary to create and promote a "virtual intelligence community," in which "every citizen is a collector, producer and consumer of intelligence". (Steele-Vivas, 1996, p. 171)

Trying to relate to the experience of different European Union member states, we observed that in Sweden, a country that promotes intelligence cooperation between the governmental, business and academic sectors, the economy is strong and the business community is highly competitive. (Porumbiță, 2014, p. 42)

Conclusions

It must be clearly understood that the world's nations are in a permanent, economic, technological or energetic competition, willing to access various natural resources in advantageous conditions, in order to enable them to successfully fulfil all the objectives associated with their national security interests.

At the same time, there are a multitude of non-state actors, with different agendas that can influence, to varying degrees, the activity of the states or the one of the private owned companies, going as far as causing them serious harm that should be prevented. Nowadays, the threat actors to the economic security are hard to be located, finding themselves both in the foreign governmental and non-governmental environment, both amongst opponents and amongst friends, allies, practically even amongst those who share common values, but have different interests.

Thus, in order to reduce the existing uncertainties and support the national security, it would be necessary to initiate and develop a sincere cooperation between the state and the private sector, cooperation that needs to be clearly regulated from the point of view of national and international law, in order to prevent potential abuses. Referring myself to the economic dimension of the security, we note that a transparent cooperation between the public and the private sector, between the national intelligence services and the business environment (mainly focused on intelligence education), between the competitive and the economic intelligence, has the potential to increase and influence the level of economic security of the state and, implicitly that of national security. It is important to mention that competitive intelligence and government intelligence use similar or even the same set of analytic techniques, applying critical thinking in their daily activity (to name just two similarities), that might represent a basis for collaboration on several directions, between these two environments. Answering the research question, in order to improve the economic security of our country, private companies and the intelligence services of the state can successfully exchange knowledge and cooperate in various relevant areas, such as counterintelligence; anticorruption; preventing and countering illegal logging; preventing and countering the destruction of hunting and fisheries stocks; counter-terrorism; information sharing on certain cybercrimes; protecting critical infrastructure; or protecting intellectual property.

In the same time, we consider that also in Romania, the intelligence services could support the private companies in different ways, such as by assisting them in setting up the competitive intelligence functions or by organizing their staff training over counter competitive intelligence, given the creation of an adequate legislation to regulate this cooperation (we believe that this demarche will also contribute to the development of both intelligence and security cultures, in the Romanian society). We estimate that since this kind of support granted to the private companies will not be free of charge, the impact to the State Budget will be a positive one. No less important, considering the case of other countries, who understand that, besides the governmental and business components, intelligence cooperation

should include an academic one, appreciating what has been achieved in this regard in our country, so far, we believe that new educational programs should be initiated, in order to prepare future Romanian graduates to protect company information, to become specialized in economic and industrial counterintelligence or economic warfare defence, in order to be able to face this new century realities.

Being a member state of the European Union, with a more secure, more competitive and stronger economy, Romania will be able to continue to contribute to the good running of the European Union, as well as to the fulfilment of all its economic, political and security objectives. In the same time, from a military perspective, as a member state of NATO, with a prosperous economy and more revenues to the State Budget, Romania will be able to contribute to the common defence expenditures with more money, being able to fulfil its plans of army endowment.

Last but not least, we must remember that, taking into account some of the possible implications of the globalization, the identification of any potential economic and industrial espionage or possible terrorist threats, for example, is not only influencing the national security of our country, but also the one of our allies and partners.

References:

1. Agheană, E. (2017). Povestea Germaniei. Comunitatea ca partener. *Revista Intelligence.* Retrieved from http://intelligence.sri.ro/povestea-germaniei-comunitatea-ca-partener/.

2. Burke, G. P. (1992). Espionage and More Benign Forms of Economic Intelligence: A Tour d'Horizon. International Security Forum apud Porteous, S. D. (1998). *Economic and Commercial Interests and Intelligence Services* in Potter, E. H. (1998). *Economic Intelligence & National Security*. Carleton University Press.

3. Calof, J., Skinner, B. (1999). Government's role in competitive intelligence: what's happening in Canada? *Competitive Intelligence Magazine*, *Vol. 2, No. 2*, 20-23.

4. Counter-espionage. (n.d.). Retrieved from https://www.sri.ro/counter-espionage.

5. Demetrescu, C. G. (n.d.). Organizarea Întreprinderilor Economice. Bucureşti: Editura Librăriei SOCEC & Co.

6. Economic Espionage: A Limited Role. *Government Executive*. (1992). apud Porteous, S. D. (1998). *Economic and Commercial Interests and Intelligence Services* in Potter, E. H. (1998). *Economic Intelligence & National Security*. Carleton University Press.

7. Economic Security. (n.d.). Retrieved from https://www.sri.ro/economic-security

8. Fota, I. (2013). Globalizarea. Bucureşti: Editura Academiei Naţionale de Informaţii „Mihai Viteazul".

9. Hohhof, B. (2014). Government and Competitive Intelligence: the wall between. Retrieved from https://www.linkedin.com/pulse/20140529202121-260716-government-intelligence-andcompetitive-intelligence-the- wall-between-the-secrets-of-companies-and-nations.

10. Neag, M., Luţac, R., & Tolontan, C. (2018). Notă SRI: Politicienii şi magistraţii care se pregăteau să pună mâna pe DNA dădeau informaţii secrete spionului chinez Wang. Retrieved from http://www.tolo.ro/2018/04/25/nota-sri-politicienii-si-magistratii-care-se-pregateau-sa-puna-mana-pe-dna-dadeau-informatii-secrete-spionului-chinez-wang/.

11. Nedelea, C. (2014). Confruntarea în intelligence: de la Războiul Rece la războiul împotriva terorismului. Bucureşti: Editura Academiei Naţionale de Informaţii „Mihai Viteazul".

12. Olescu, E. (2012). Presupus caz de spionaj al zăcămintelor din Moldova Nouă. Retrieved from http://www.bursa.ro/presupus-caz-de-spionaj-al-zacamintelor-din-moldova-noua-187825&s=print&sr=articol&id_articol=187825.html.

13. Petrescu, Stan. (2011). Despre intelligence: spionaj-contraspionaj. Craiova: Sitech.

14. Porumbiţă, M., Han, L., & Stan, M. (2014). Organizaţii de Intelligence. Bucureşti: Editura Didactică şi Pedagogică.

15. Potter, E. H. (1998). Economic Intelligence & National Security. Carleton University Press.

16. Sava, I. N. (2005). Studii de Securitate. Bucureşti: Editura Centrului Român de Studii Regionale.

17. Sebe, M. M. (2010). Intelligence guvernamental şi privat pentru competitivitate şi securitate naţională. Bucureşti: Editura Academiei Naţionale de Informaţii „Mihai Viteazul".

18. Security strategy. (n.d.). Retrieved from http://www.sri.ro/security-strategy.

19. Steele-Vivas, Robert David. (1996). Creating a Smart Nation: Strategy, Policy, Intelligence and Information. *Government Information Quaterly.* Retrieved from http://www.oss.net/dynamaster/file_archive/040320/dc199ef0d5d4da35fbc9b803ad3dfe6b/OSS1995-02-21.pdf.

20. The White House. (2017). National Security Strategy of the United States of America.

21. Whitney, C. (1993). Germany Finds That Spies Are Still Doing Business. *New York Times.* apud Porteous, S. D. (1998). *Economic and Commercial Interests and Intelligence Services* in Potter, E. H. (1998). *Economic Intelligence & National Security*. Carleton University Press

ACADEMIC FOCUS

SBSR Program, 2020 edition: Young Leaders for Democracy and Security. A training program for young leaders on how to build secure societies in the Black Sea Region and the Balkans (June 2-4, 2020, Constanţa, Romania)

Program: *Security in the Black Sea Region. Shared Challenges, Sustainable Future Program* is an interactive and practical training program dedicated to young and emerging leaders in the Black Sea Region and the Balkans. Its aim is to foster and enhance leadership, conflict resolution, critical thinking, and strategy and cooperation skills.

Organizers: The program, at its 7th edition, is organized by the "Mihai Viteazul" National Intelligence Academy, Romania in partnership with Harvard Kennedy School of Government, US. It stands under the high patronage of the Romanian Presidential Administration. The 2020 edition shall be dedicated to training young and emerging leaders on how to build secure societies in the Black Sea Region and the Balkans.

Special mentoring feature: The program shall be held at Hotel de Mar, in Constanta, Romania (June 2-4, 2020), during **the Black Sea and The Balkans Dialogue Week**, as a back to back event with the *New Strategy Center*'s **Black Sea and the Balkans Forum**, to be held in the same venue (June 4-6, 2020). The back to back format provides the opportunity for young and senior leaders in the two regions to meet, share ideas and debate on how to build secure societies in the future. It will include a special mentoring session with senior policy makers present at the Forum, bridging vision across generations of leaders.

Program Statement: **#teamwork #initiative #creative thinking #gender balance #mutual understanding. #inter-faith dialogue #respect. #equity**

Being addressed to the Black Sea Region and the Balkans emerging decision makers in the fields of intelligence, security, foreign affairs and public diplomacy, one of the main aims of the program is to create the right framework in which young generations can interact freely and creatively, as well as debate with senior stakeholders, academia and high level officials, in full respect of each other and of potentially diverging interests, to promote mutual understanding and respect. Acknowledging multiculturalism, diversity and inter-faith acceptance as tools to transform societies, the training program aims to contribute to accelerating the pace at which gender balance, community cohesion and inter-faith acceptance is reached in the Black Sea Region.

The 2020 edition of SBSR, ***Young Leaders for Democracy and Security***, combines formal and informal education strategies to foster learning by doing and ownership. The program of academic lectures on policy, public diplomacy, security and cultural strategies is complemented by roundtables with NATO and EU officials, a decision making exercise, a spotlight event, life skill sessions, an ad-hoc campfire and networking events.

Eligibility:

Young aspiring leaders in intelligence, security, foreign affairs and public diplomacy, under 35 years old; early and middle-career professionals and PhD students with working knowledge of English. Experience in international relations, intelligence, security and/or diplomacy is considered a plus.

Strategic partnership project within
ERASMUS+ Program
AGREEMENT No. –
2018-1-RO01-KA202-049449

MIND THE GAP IN MEDIA COVERAGE AND STRATEGIC COMMUNICATION IN CASE OF SECURITY THREATS – THE DEVELOPMENT OF CRITICAL THINKING AND RESPONSIBLE REACTION

(October 1st, 2018 –
September 30th, 2020)

CRESCEnt project addresses the challenge of social polarization created by the propagation of disinformation and fake news. It is a proven fact that fake news have created in Europe, and in the three countries participating in the project, an acute miscommunication and lack of trust between the two targeted professional categories. As the media has been pressed into reaching large audiences, institutional spokespersons were forced into communicating what is necessary and not divulging aspects which could jeopardise security investigations and public safety. A gap of trust and efficient communication was, thus, created and later on widened by the phenomenon of fake news. While it is indeed the media professionals that shape the way information is delivered to the public, they themselves might get trapped in particular "narratives" and share common mental frames. Recognizing that the media professionals are themselves the locus of potential influence by external actors is crucial to developing strategies to combat misinformation and hostile influence. CRESCEnt aims to address this divide through innovative solutions and multiplication of best practices of both spokespersons and journalists.

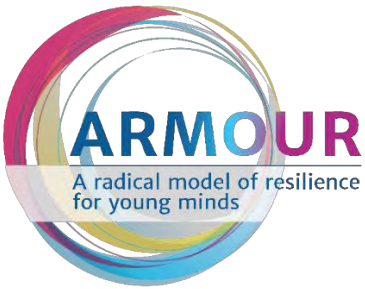
CRESCEnt project creates a training platform and a set of communication and cross-sectorial strategic communication instruments, which aim to capacitate institutional spokespersons and journalists from security and LEA fields, in order to use media reporting to the public in a conscious and ethical manner. CRESCEnt's main target group consists of spokespersons in the field of national security and LEAs. The secondary group is represented by (young) journalists who are active in the field of security.

Participating organizations are: "Mihai Viteazul" National Intelligence Academy (MVNIA) – Romania; University "Rey Juan Carlos" (URJC) – Spain; Kentro Meleton Asfaleias (KEMEA), Centre for Security Studies – Greece; Ministry of Internal Affairs, Directorate for Information and Public Relations (MAI-DIRP) – Romania.

Objective of the project are:

- to develop a toolkit of techniques, methods and instruments for institutional spokespersons and journalists who communicate on issues related to security and law enforcement, as support in their professional activity;
- to enhance key-competences and skills of the spokespersons and journalists so that they become resilient to fake news, build an ethics of reporting, perform double fact checking, provide and obey ethical grounds in handling sources, report security threats and handle truth for the preservation of democracy and the rule of law.

The CRESCEnt project is part of the ERASMUS+ program and it is funded by the European Commission. See more about the project on the official website: https://crescentproject.eu.



A RADICAL MODEL OF RESILIENCE FOR YOUNG MINDS – ARMOUR

Grant Agreement No. 823683
(January 1st, 2019 – December 31st, 2020)

The Euro-Arab Foundation leads ARMOUR (*A Radical Model of Resilience for Young Minds*) consortium and the project aiming to **address the social polarization caused by** the adoption and spread of **extremists ideologies** by creating an interdisciplinary **learning model that helps individuals and communities develop resilience** to the specific ideologies and behaviours of violent extremism.

The **ARMOUR**'s consortium, led by the Euro-Arab Foundation, is also made up of the Centre for Security Studies – KEMEA (Greece), the "Mihai Viteazul" National Intelligence Academy (Romania), SYNYO GmbH (Austria), the Italian Ministry of Justice, Agenfor (Italy), LIBRe Foundation (Bulgaria), the University of Malta (Malta) and the University of Groningen (Netherlands).

ARMOUR Project aims to address **societal polarization** via strengthening resilience of individuals, communities and vulnerable groups (such as children, youth etc.) to polarisation, and to promote **interaction and cooperation between different local actors** from public sectors, i.e. law enforcement, social services etc., that specialise in working with vulnerable groups in preventing extremism through development of cooperation models. The project will design and create a **Toolkit for first-line practitioners** to employ in **reducing polarization among children and youth**.

The Toolkit, capitalizing on previous work carried out by project partners, takes the form of **experimental laboratories** (experimental labs) which together work towards: strengthening individual capacity to resist push and pull factors of radicalization; creating community empowerment and resilience to social polarization and violent

extremism and assisting states deploy proportional responses against provocations and latent conflicts. The model will then be promoted through a social media campaign.

The **expected impact** of the project covers the following aspects:

- **Increasing awareness and capacity of first-line practitioners:** ARMOUR achieves this through the experimental labs and the related training programme. The first tool will help practitioners better understand and identify instances of radicalization and polarization among children and youth while the second one will help them improve their ability to use the project toolkit.
- **Promoting interaction and cooperation among different stakeholders:** ARMOUR achieves this by organizing the experimental labs in which practitioners and members of vulnerable communities have trusted interactions.
- **Promoting the views of moderate voices** by engaging with the silent majority and integrating them into the experimental lab.
- **Developing and promoting concrete tools targeting vulnerable groups:** the experimental lab combined with the best practices identified in the project and the online campaign are concrete tools which key actors can use when working with vulnerable youth.

The project is financed by the Internal Security Fund, a funding package of the Directorate-General for Home Affairs (European Commission) to promote the implementation of the Internal Security Strategy, law enforcement cooperation and the management of the Union's external borders. See more about the project on the official website: https://armourproject.eu/a/privacy-policy.

CALL FOR PAPER ROMANIAN INTELLIGENCE STUDIES REVIEW

`Mihai Viteazul` National Intelligence Academy, via its National Institute for Intelligence Studies, publishes the *Romanian Intelligence Studies Review* (RISR), a high quality peer reviewed and indexed research journal**, edited in English and Romanian twice a year.**

The aim of the journal is to create a framework for debate and to provide a platform accessible to researchers, academicians, professional, practitioners and PhD students to share knowledge in the form of high quality empirical and theoretical original research papers, case studies, conceptual framework, analytical and simulation models, literature reviews and book review within security and intelligence studies and convergent scientific areas.

Topics of interest include but are not limited to:

- Intelligence in the 21st century;
- Intelligence Analysis;
- Cyber Intelligence;
- Open Source Intelligence (OSINT);
- History and memory in Intelligence;
- Security paradigms in the 21st century;
- International security environment;
- Security strategies and policies;
- Security Culture and public diplomacy.

Review Process: RISR shall not accept or publish manuscripts without prior peer review. Material which has been previously copyrighted, published, or accepted for publication will not be considered for publication in the journal. There shall be a review process of manuscripts by one or more independent referees who are conversant in the pertinent subject area. Articles will be selected based on their relevance to the journal's theme, originality and scientific correctness, as well as observance of the publication's norms. The editor evaluates the recommendation and notifies the author of the manuscript status.

The review process takes maximum three weeks, the acceptance or rejects notification being transmitted via email within 5 weeks from the date of manuscript submission.

Date of Publishing: RISR is inviting papers for No. 23 and 24 and which is scheduled to be published on June and December, 2020.

Submission deadlines: February 1st and July 1st

Author Guidelines: Author(s) should follow the latest edition of APA style in referencing. Please visit www.apastyle.org to learn more about APA style, and http://www.animv.ro for author guidelines. For more details please access the official website: **rrsi.ro**

Contact: Authors interested in publishing their paper in RISR are kindly invited to submit their **proposals electronically in .doc/.docx format at our e-mail address rrsi@sri.ro, with the subject title: RRSI article proposal.**

Appearing twice a year, the review aims to place debates in intelligence in an institutional framework and thus facilitating a common understanding and approach of the intelligence field at national level.

The target audience ranges from students to professionals, from the general public to those directly involved in intelligence research and practice.

ISSN - 2393-1450
ISSN-L - 2393-1450

"MIHAI VITEAZUL"
NATIONAL INTELLIGENCE ACADEMY

National Institute for Intelligence Studies

20, Odăi Str.
Bucharest 1 - ROMANIA
Tel: 00 4037 7721 140
Fax: 00 4037 772 1125
e-mail: rrsi@sri.ro

www.animv.ro
www.rrsi.ro