NEW CHALLENGES ON THE INTELLIGENCE FRONTLINE – A PRACTITIONER'S PERSPECTIVE

Florian COLDEA[*]

Abstract

This century has come with different types of challenges in security matters that set a new security agenda for multiple fields, including intelligence. We all live in a growingly complex IT ecosystem, where the availability of the technology is pushed to lower levels, the security of information is fragile, and the citizens change the ways they communicate with one another and with states and governments. The technology-related change is affecting the intelligence agencies ability to deal with some of the most important threats, ranging or coming from the cyber arena, hybrid warfare, large scale migration flows, terrorism, counterespionage and other. Tackling these phenomena is not an easy task for the intelligence field requiring a comprehensive and reinforced cooperative approach, mutual support and assistance, doubled by the responsibility at state levels in decision making.

Keywords: challenges, gaps, security agenda, technology, innovation, way forward.

Introduction

The Problem. The XXI century comes in front of us with some different types of challenges in security matters. From the already "old" Y2K computer rollover problem in 2000, to the major and continuous terrorist plots in many western cities, to a series of disasters related to natural phenomena or large scale migration, to the tremendous security issues raised by the "Internet of things", people, states and societies are confronted with a new security agenda, in many ways different to what we experienced in the 20th century, with its nearly "frozen" set of threats.

Some specific situations. That new security agenda and its challenges have some specific information related aspects. In most of the cases, the threat is directly related to information (Jouini, Rabai & Aissa, 2014), as in all that

[*] Romanian Intelligence Service.

series of cyber attacks against state or private owned information systems. In others, the leaders or crisis managers need critical information that they cannot obtain because of the lack of a solid institutional or organizational infrastructure (Suchan, 2002).

Other challenges require a smart mix of secret information (from human or technical sources) and complex data already available, but not really integrated in a viable intelligence system (Delaforce, 2013).

People & administrations meet technology

The advance in communication technology in the early part of the twenty-first century have fundamentally altered **the way that ordinary citizens communicate with one another and with their states & governments**. This has demonstrably changed the character of social relations in modern societies, patterns of commerce, and relationship between the citizen and the state (Goldsmith & Crawford, 2014). The ubiquity and availability of technology is changing the face of security and privacy, and intelligence professionals must understand the current trends if they want to meet the new challenges.

As **technical collection and storage has become more accessible** to a greater range of government departments, so the number of mass population databases and the like have emerged that lay bare a wealth of sensitive information to different state agencies and those they engage with in the name of security or, more often, in the name of service delivery.

These agencies are not limited to intelligence and policing agencies – as most people still believe –, but also extend to include local administration and tax collection authorities, for example. This is a large extension of the powers granted to agencies not engaged in security and policing work.

The use to which data is put by different domestic authorities has caused considerable concern to most of privacy campaigners (being as they include information on biometrics, images, money transaction records, medical records etc., among many classes of information).

But is **the leakage & collection of this type of data by the private sector** (and the use it might be put to), and the number of access points where data could be illegally accessed by adversaries, that **is a separate and larger cause of concern**.

To sum up, if the availability and usability of the technology is pushed to lower levels, on the contrary, the knowledge needed in order to secure information is not being pushed down, not at the same speed, at least. In this manner, the security of information is more and more fragile, in direct proportion to the use that is made by states and, even so, by the private sector.

The presence of that entire technological infrastructure creates what we could call an "ecosystem", in essence, a 24/7 operating system in which servers, networks and apps are sending and receiving data to/from some other servers, networks and apps – all hopefully in the interest of states, companies, and the people or clients they serve.

States loses monopoly over technology: the gap challenge

The last decade we witnessed a shift in the technological paradigm, generated by an exponential increase in the budgets that private actors dedicate to new technologies, both for development and integration in the "business as usual" process – leaving behind the former "stars", the state actors. It has become clear that states are no longer the main drivers in the technology development, and institutions must adapt in order to keep the rhythm now is imposed by private actors and to respond to the changing expectations of the society. **This gap** between technological advancement and state capability represents **a new and strategic vulnerability** – as it challenges the institutional ability to use the latest advancement in technology, even in major crisis situations.

Andrew Parker, Director General of the MI5, points out that „**the chronic yet critical challenge we face comes from technological change**" (adresa from January 8, 2015), because the technology-related change is affecting our ability to deal with some of the most important threats.

This is not a surprise: the ability to access terrorist communications is vital to intelligence agencies ability to keep their countries safe. The internet has changed so many aspects of our lives – better in so many ways, revolutionizing commerce and communication, providing multiple choices and better access to information for us all. But also, as the examples showed early enough, it offered the same advantages and opportunities to terrorists too (Weimann, 2004).

All the greatly praised virtues of the Internet – easy access, no or little regulation, large and global potential audiences, fast flow of information, and much more – have been turned to work in the advantage of groups determined to terrorize societies in order to achieve their goals. In these days, all active terrorist groups already have an established presence on the Internet, sometimes in a very dynamic way: websites, groups and networks suddenly emerge, frequently modify their formats, and then swiftly disappear – or, in many cases, seem to disappear by changing their address but retaining similar content or membership.

They use it to spread propaganda, to radicalize impressionable individuals, to arrange travel, to move money; but most of all to communicate with one another, to plan and organize. They use the same communications

tools as the rest of us. But technological and market changes risk closing off areas where we need to be able to operate.

The dark places from where those who wish to harm us can plot & plan are increasing. So, we – the state, societies, and agencies – need to keep the rhythm and not allow this technological gap to become a new territory and source of not-manageable threats.

Threats and technological change

The cyber "arena". Nowadays a broken or failing USB stick could induce more damage than a classical bomb or missile. The cyber threat not only changes the face of warfare, but also poses great risks to states and citizens. Cyber warfare is a relatively new phenomenon, its emergence being justified by our growing dependence on the cybernetic infrastructure and facilities, but also by the very low cost of transforming this tool intended for work and communication to an immaterial weapon that has a highly offensive potential. There are multiple changes in the conventional paradigm of the battlefield, and this cyber approach seems to operate a shift from means to end (Sharma, 2009) – a very good reason to understand and keep up with the permanent evolutions that take place every day in IT.

From a professional perspective, these IT evolutions must be viewed in relation to what already represents a challenge for the security field, and within this perspective it is clear that they become a new trigger for both older and recently discovered threats (espionage, sabotage, disinformation, energy, etc). It is also commonly accepted that we witnesses the creation of a new so called "confrontational arena" (Kostopoulos, 2008, pp. 165-169) – the cyberspace – with its own new kind of vulnerabilities, risks and opportunities.

Cyber attacks happens every minute in the world and even if only a very small part of them have **the potential to harm national security**, the consequences already proved to have the potential to be disastrous.

For all intelligence agencies it is vital to keep pace in this new arena, to remain competitive in their ability to tackle the challenges coming from it. The SRI expanded his cooperation with his partners (both at national and international levels) and created a Cyberint Center[1] to help protect and ensure the needed resilience of this vital core of critical infrastructure of the state and society, the IT systems.

As the doctrine in this field tend to change with every major attack or "leapfrog" in technology, intelligence agencies need to operate under a flexible and upgradable set of norms that empowers them to efficiently respond to

[1] More details on the set up of this specialized structure available on the official website, http://www.sri.ro/cyberintelligence-en.html.

new cyber threats, but within a clear legal framework that doesn't expose neither the citizens, nor the state and the institutions.

Counterintelligence in the information era. The rapid pace of technology has brought new problems and opportunities for the agencies and agents involved in counterintelligence activities. There is an incredible amount of information already available on internet, and relatively accessible to other agencies or even "ambitious" individuals, giving the possibility to access or aggregate secret information. Ten years ago, a newspaper was able to create a list of thousands of CIA agents, dozens of internal phone numbers and even more classified facilities, home addresses and cover names simply by thoroughly scanning commercial databases that were available online (Crewdson, 2006).

If, usually, technology is supposed to facilitate the rapid and large distribution of information, the role of the counterintelligence is to block the access to one's agency or state information. It is very important that CI rapidly adapt to the new operational conditions implied by the information age.

But this responsibility is not to be placed only on the shoulders of intelligence officers/agencies: partly because some of them are not technically prepared to ensure high levels of security against worldwide skilled hackers or armies of hackers, partly because most agents and information are vulnerable by reasons beyond their responsibility, such as indexation in multiple administrative databases, facial recognition facilities, poor security design of critical IT infrastructure etc.

Challenges must be approached at a wider level, by state or even allied policies, articulated into a vision that involves integrated approaches regarding people, processes and infrastructures, a vision that takes into account classical human threats and the ever rapidly growing technical threats. A new mix of resource management and training programs is needed in order to out pass the current organizational and cultural obstacles that still separate counterintelligence from intelligence and other types of activities relevant to the outcomes. Modern (and often expensive) technologies are required to enhance CI wide spectrum of operations. And last but not least, there is a vital need in the overall process, namely to obtain and maintain the trust of citizens, that our counterintelligence policies are structured and implemented in a strictly legal framework, free of suspicion and fear.

Hybrid warfare may be a *new challenge*, but its main elements are not really new (Wilkie, 2009). We all have seen before energy security used as a political weapon, or conventional military maneuvers combined with powerful cyber attacks and increased propaganda spread through new

media. I think this "not really new" idea should be further debated among military thinkers, as we see that the conflicts of our times are getting more and more complex.

Although there is no unanimously accepted definition, we can easily understand **hybrid warfare as a "cocktail" or a "mix"** of classic military forces, insurgencies, terrorism, organized crime, and advanced technologies. This type of warfare can include violations of international laws, often by „private" actors, backed by states with questionable agendas. All this may be mixed together in different settings and proportions and, even more, any ingredient may be in or out at different phases of the hybrid warfare.

So is there anything new with the hybrid war? It may well be the fact that recently we have witnessed a use of its main components on a larger scale and in a more coherent manner. That's what is new: the *scale* and the *focus*. And the Ukrainian conflict almost represents a "case study" opportunity for any security practitioner interested in this type of warfare.

As Clausewitz (1989, p. 593) found: "every age has its own kind of war, its own limiting conditions, and its own peculiar preconceptions". And, as such, even if the concept of hybrid war is not really new, the intelligence and security professionals must take into account that its means are growing increasingly sophisticated and deadly, and require a proper response.

This may mean that in our constant effort to update the principles and theories of war, ultimately we have to see what parts of them still remain constant. In this field there is no "cycle" that conducts to new revolutionary panacea every decade, but permanent and incremental changes are part of business as usual in security matters. True "revolutionary paradigm changes" are less prone to occur than most conference speaker seem to believe.

At the NATO level, as I already explained in another paper (Coldea, 2016) – under the evidence of cyber attacks that hit Estonia in 2007 – the subject was discussed for the first time in January 2008, and further debated at the NATO Summit held in Bucharest in April 2008.

Terrorism proved to be a multilayered and very dynamic phenomenon, remaining one of the main threats to national and international security – mainly because it constantly traversing a changing curve. What we believe to know about this phenomenon at a certain moment may not be well suited to counter it in the future, because if the root causes remain relatively constant, the modus operandi and the tactics, the structure and organization constantly evolves. It is what makes terrorism a permanent challenge for intelligence agencies and such a vast topic of research for academia.

The constant evolution of terrorism pushed this phenomenon under the conceptual umbrella of hybrid threat, as it clearly is the case with the

Daesh and its "state like" ambitions – raising new challenges for all state institutions and security practitioners. Another example is the growing flow of foreign fighters and returnees to/from conflict areas, mainly Iraq and Syria (*Addressing the Foreign Terrorist Fighters Phenomenon from a EU Perspective*, decembrie 2014) – a flow not only of persons, but also of military skills and radical ideas, logistical and financial support, terrorism promoters and even perpetrators.

To put things in perspective, to some extent similar to the hybrid issue, it must be said that the foreign fighters problem is not a new phenomenon. In XX century dozens of insurgencies have gone international and there have been foreign fighters in many modern civil wars, many voices counting English poet Lord Byron as a foreign fighter in Greece in the 1820s (Malet, 2010, p. 101). What is new in present times is the scale of the threat raised with the outbreak of civil war and sectarian violence in Syria, Iraq, Libya, and other countries.

Tackling these phenomena is not easy, as it has become more and more clear in the recent years. It **requires a comprehensive and cooperative approach**, as it is an international rather than a national issue and can only be addressed effectively by common efforts of more than a few countries and/or agencies. We have seen that after each major attack (Paris 2015 and 2016, Bruxelles 2014 etc.) the respective national judicial norms are updated, mainly by framing new terrorist offences. It is a common and foreseeable reaction to the growing threat, but that may also create some new risks related to the lack of common standards or even prosecution and criminalization gaps across different but similarly exposed countries.

In that context, the need to enhance international cooperation has become more and more evident, and may be further reinforced by multi-disciplinary approach (judicial, intelligence…). None of us can deal with this threat alone, so close and applied cooperation is required.

Immigration. The number of immigrants and refugees was raising sharply in 2015 and has become quickly a prominent matter on European political and security agendas, confronting the decision makers with key issues regarding: the impact on the transit and destination countries (*Countries of transit ...*, 11 septembrie 2015), the impact on the common European ties and solidarity (Goldner Lang, 2015), the measure in which the globalization has become a catalyst for large population movements, what respective roles for state institutions and civil society etc.

From a security perspective, the main error is to think and frame this issue in limited domestic terms, as it actually is a pan-European problem caused by a pan-Arab arch of conflict and instability. Across the European

countries, the policy issues and the main items of debate are very similar, in some cases overlapping sensitive matters as security, identity and ethnicity. This proves, once more, that it is a common issue requiring solidarity among member states in reciprocal support and assistance.

If we want to keep things in perspective, while the truth is that no one knows what will happen to immigration trends on the short and medium run (the long term probability being that small wars and the urbanization trend of the world's population will keep the immigration numbers high), it is the common responsibility of states that will help us to deal with the issue and to protect our national and regional security.

The perspective of "high numbers" generates new risks, also relevant for the law enforcement agencies and the security and information services. These institutions must adapt and adjust their resources (human and financial) and need to operate in an updated legal framework.

Conclusions of the way forward

The rhythm of technological change and innovation had left behind regulation, and oversight in the past decade. Without a serious update of the law and oversight regarding these technologies and practices, and without honest and open debates over the extent of surveillance by public and private sources, this gap will become even wider.

States and societies must adapt their reflexes to this world of growing interdependence and interaction even between apparently distinct issues such as terrorism and health, and between actors, such as people, government and industry.

The key challenge here is **to build state capabilities,** to set up and support solid institutions, based on democratic principles, and always keeping an eye on their professionalism, accountability and integrity.

I believe it is our responsibility, as intelligence professionals, to **keep pace with these rapid developments** in the actual volatile security environment and to propose **new imaginative solutions** in order to ensure and protect the security of the citizens.

All these challenges are to be **better understood by common efforts** (among decision-makers, practitioners, academics) so we can achieve a deeper knowledge of the matters and we can recommend viable solutions. This manner of approaching difficult subjects favors **the exploration of new perspectives** and paradigms

We must continue to search for new ways to manage all these relationships **at a time when the public demand for information and transparency is higher than ever**.

References:

1. *Address by the Director General of the Security Service, Andrew Parker, to the Royal United Services Institute (RUSI) at Thames House*, January 8, 2015, available on https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/director-generals-speech-on-terrorism-technology-and-accountability.html.
2. *Addressing the Foreign Terrorist Fighters Phenomenon from a EU Perspective*, Global Center on Cooperative Security, Human Security Collective, and International Centre for Counter-Terrorism – The Hague, Policy Brief, December 2014.
3. Coldea, Florian, (2015), *Building national capabilities and countering hybrid threats: lessons learned*, Key Note Speech at NATO Advanced Research Workshop on *Countering Hybrid Threats: Lessons Learned from Ukraine*, Bucharest, 2015 September 28-29th.
4. *Countries of transit: meeting new migration and asylum challenges*, Council of Europe Committee on Migration, Refugees and Displaced Persons, Doc. 13867, September 11, 2015, available on http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=22017&lang=en.
5. Crewdson, John, (March 12, 2006), *Internet Blows CIA Cover*, in Chicago Tribune, available on http://articles.chicagotribune.com/2006-03-12/news/0603120396_1_agency-employees-or-operatives-cia-director-porter-goss-two-dozen-secret-cia.
6. Delaforce, Ruth, (2013), *Public and private intelligence: historical and contemporary perspectives*, în *Salus Journal*, Issue 1, Number 2, available on http://www.salusjournal.com/wp-content/uploads/sites/29/2013/03/Delaforce_Salus_Journal_Issue_1_Number_2_2013_pp_21-39.pdf.
7. Goldner Lang, Iris, (2015), *The EU Financial and Migration Crises: Two Crises – Many Facets of EU Solidarity*, in E. Dagilyte & E. Küçük (eds.), *Solidarity in EU Law: Legal Principle in the Making*, Edward Elgar Publishing.
8. Goldsmith, Stephen, Crawford, Susan, (2014), *The responsive city. Engaging communities through data-smart governance*, San Francisco, Jossey-Bass.
9. Jouini, Mouna, Rabai, Latifa Ben Arfa, Aissa, Anis Ben, (2014), *Classification of Security Threats in Information Systems*, Procedia Computer Science, Volumul 32, pp. 489–496.
10. Kostopoulos, George K., (2008), *Cyberterrorism: The Next Arena of Confrontation*, Communications of the IBIMA 6(1), pp. 165–169, available on http://www.ibimapublishing.com/journals/CIBIMA/volume6/v6n25.pdf.
11. Malet, David, (2010), *Why Foreign Fighters? Historical Perspectives and Solutions,* Published by Elsevier Limited on behalf of Foreign Policy Research Institute, Winter 2010.

12. **S**harma, Amit, (2009), *Cyber Wars: A Paradigm Shift from Means to Ends in The Virtual Battlefield: Perspectives on Cyber Warfare*, Proceedings 2009, NATO Cooperative Cyber Defence Centre of Excellence, available on https://ccdcoe.org/sites/default/files/multimedia/pdf/01_SHARMA_Cyber_Wars.pdf.
13. Suchan, William, (2002), *The organizational information infrastructure maturity model*, AMCIS Proceedings, Paper 295, available on http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1654&context=amcis2002.
14. Von Clausewitz, Carl, (1989), *On War,* Princeton University Press.
15. Wilkie, Robert, (2009), *Hybrid Warfare: Something Old, Not Something New*, în Air & Space Power Journal - Winter 2009, available on http://www.airpower.maxwell.af.mil/airchronicles/apj/apj09/win09/wilkie.html.
16. Weimann, Gabriel, (March 2004), *How Modern Terrorism Uses the Internet*, US Institute of Peace, Special Report 116, available on http://www.usip.org/sites/default/files/sr116.pdf.