A FAUSTIAN PACT: THE REGIME OF TRUTH WITHIN NATIONAL SECURITY DOCUMENTS IN ROMANIA AND GERMANY

Iulian DICULESCU-BLEBEA*

Abstract

The main purpose here is to open an academic door towards a very inciting and promising nexus, to launch an invitation to scholarly "occupy" the common niche of truth and security – which appear to become increasingly relevant, especially against the background of the currently re-emerging ideas and debates around post-, hybrid-, fake- and many others alike. This study focuses on how the idea of (a crisis of) the regime of truth is addressed, as a whole or through some of its core elements, in a series of strategic documents. It investigates whether and how it is framed as a matter of security, showing the official approaches in which the Romanian and German authorities frame and tackle the problem in the particular instances given by their respective security strategies. The hermeneutical approach of these documents, based on a Foucauldian conceptual toolbox and his archaeological approach for the „questioning of the document", with accent on their specific perceptions and understandings, on their actual and latent content, indicates how and in what a surprisingly extensive manner these strategies address issues related to the core elements of a regime of truth. Although the selected security strategies approach the idea of truth in an indirect and rather implicit manner, they stand nevertheless into the matter through a consistent use of semantical, ideatical or contextual substitutes, and also through narratives on related problems. These official documents contain an impressive body of statements and practices that concern the dynamics by which truth related issues are addressed (understood, framed and managed) through security ideas and processes within the Romanian and German milieus.

Keywords: *(regime of) truth, security, crisis, order, rules, normalcy, Romania, Germany.*

* PhD stud. in International Criminology, Hamburg University, Germany, iulian.diculescu-blebea@studium.uni-hamburg.de

More than just formalities, Foucauldian "monuments"

In order to evaluate if and how truth is treated as a matter of security, I started by looking at a number of key documents, namely top level strategies and programs that are produced, usually, within a collective bureaucratic process and then assumed or approved at the highest political level. For a meaningful comparative approach, two very similar types of such documents, adopted in Germany and Romania, will be further analyzed. First, the national security strategies: the *2016 White Paper "On German Security Policy and the Future of the Bundeswehr"* and *The National Defence Strategy 2015-2019 "A Strong Romania within Europe and the World"*. Secondly, the cyber security strategies: the *Cyber Security for Germany 2016* and *The Romanian Cyber Security Strategy 2013*.

The documents, in their wider variety of forms – letters, transcripts, files, tickets, laws etc. – appear as ubiquitous instruments of many social organizations. This study assumes a Weberian point of view on the "modern officialdom" and the idea that its functioning is "based upon written documents ('the files')" (Weber, 1968, pp. 956-958 and 999-1001). The official documents represent a very useful starting point, as they convey the formal approaches at work in a society, the approved or authorized ways of thinking and acting, often being able to confer legitimacy or authority. Also, the fact that they are written has a special relevance in our modern culture, as the written word ambitionates or at least is expected to demonstrate a certain resilience in time, bearing a certain "symbolism of permanence" (Navaro, 2007, p. 84). As Hodder says, this kind of "mute evidence […] unlike the spoken word, endures phisycally" (Hodder, 2012, p. 171). Despite the relatively bureaucratic process, their authors most often hope to cover key issues of the matter they try to address, to make statements that would be approved or at least obeyed, that would be judged as truthful or at least appropriate. The fact that such documents mobilize both ideas and actors in a temporally remanent form, as implied since the well-known Latin adage *scripta manent*, makes them sources of first interest when it comes to researching how specific issues are understood, framed and governed.

Foucault also raised this issue of the "questioning of the document" and emphasized an essential shift in perspective from understanding documents and what they say as a basis for the reconstitution of the milieu/past from which they emanate (the memory task), to trying to "work on it from within and to develop it" and to "define within the documentary material itself unities, totalities, series, relations" (Foucault, 2002, pp. 7-12) (the archaeological task). As he wrote, „we must grasp the statement in the exact specificity of its occurrences; determine its conditions of existence, fix at least its limits, establish its correlations with other

statements that may be connected with it, and show what other forms of statement it excludes" (Foucault, 2002, p. 31). The Foucauldian approach of the documents is archeologically and it is realized by "turning documents into monuments" which means "nothing more than a rewriting… a regulated transformation of what has already been written… the systematic description of a discourse-object" (Foucault, 2002, p. 157).

Implicit but extensive approach – the truth and nothing but the whole system of it

At a first sight it would appear as quite an unexpected thing for such official documents – high level strategies and programs – to refer to the problem of truth. According to the usual common sense, truth seems to belong to another register of ideas and thinking, more philosophical and less strategic, rather ideatical than formal or bureaucratic. Nevertheless, a hermeneutical approach of the selected security strategies and governing programs, with focus on their specific perceptions and understandings, on their actual and latent content, indicates how and in what a surprisingly extensive manner these documents address issues and matters related to the core elements of a regime of truth.

By regime of truth I point, in a clear Foucauldian line, to something conceptually wider than the truth by itself, to a larger framework of many constraints within which truth is produced and that, alongside with a number of enduring common features, has also specific elements for each society and period of time. According to Foucault, this regime is a systemic arrangement that concerns: 1) the acceptable types of discourse; 2) the mechanisms and instances for separating true and false; 3) the means by which each is sanctioned; 4) the techniques and procedures valued in the acquisition of truth, and 5) the status of those establishing what count as true (Foucault and Gordon, 1980, p. 131). Looking at these elements it is easier to understand that most of the battles "for" truth, or at least "around" it, are not actually conducted "on behalf" of the truth directly, but concern rather the status and the role it plays, or the rules that separate the true and false, in a word, its regime. Most of this regime is not as much about the truth itself, as it is about nearby social acts, ideas and practices.

One of the very first things to underline is that all the cited documents address the idea of truth in an indirect and rather implicit manner. There is no explicit reference to the word "truth" as such, as a common noun, nowhere in the texts under analysis, and only in rare instances appear some direct declensions of it, mainly as adverb or adjective in rather linguistic constructions: "it is true that…" (Germany *White Paper*, 2016, p. 64), "true mutations of…" (Romania *Cyber*

Security Strategy, 2013, p. 4). Nevertheless, the documents stand into the matter through a consistent use of semantical, ideatical or contextual substitutes. And by doing so they get to deal with aspects that constitute or contribute to the systemic arrangement of the main constraints/conditions that counts for the establishment and circulation of truth within the Romanian and German political and security milieus. The truth is not approached directly, but through different substitutes or, mostly, through narratives on related problems, such as: the knowledge as the main way to track and acquire the truth about *dangers*, seen as a central security need and structured in an almost axiomatic way; the ubiquitous crisis of a deeply challenged social order that affects our lisibility, understanding and handling of key information or social realities; the grey spaces, uncharted or porous, such as the cyberspace, where true and false as well as their respective agents are hardly distinguible; the security culture as an important complement to knowledge, including a constant awareness and "appropriate" sets of ideas, practices and behaviours for the citizens; the security understood as human made normalcy, with consequences on related truth seeking, establishing and telling practices; and many others, such as the information, the data, the seal, the safe use, the certified product etc. These are treated within the next sections of this study and most are common for both Romania and Germany, except for some specific national elements.

Altogether the documents converge and create a rich official metanarrative that frame and prescribe the acceptable discourses on how the world *actually is* (crisis, unsettlement, mutations), on how it *should be* (order, stability, normalcy) and on what it *should be done* (to know, to behave, to care...) according to certain conditions and rules. There is a clear tension between description and prescription, between the actual state of German and Romanian security milieus (abnormal) and the ideal (yet "normal") , and this gives to the official meta-narrative a sense of crisis and exceptionality that empowers the actional dimension of these documents, the "should be done" part.

In addition, all these strategies and programs count among the highest level national documents and, as such, they have an impact on major social settings and practices, and also a strong constitutive effect: they establish key policy and security objectives, they offer guidelines and instructions *for* (and, of course, *about*) the security apparatus, they indicate the acceptable discourses about the security environment, they also provide the highest political narrative on security issues and this narrative also addresses matters that are relevant for the professional and social handling of truth.

Some of the values and principles whereupon the whole strategic act is claimed to be grounded, as well as the security interests and objectives are clearly related to the general idea of truth and very important for the narrow

institutional and the wider social handling of it. In the Romanian case for example, the value of "dignity" (Romania *National Defence Strategy*, 2015, p. 7) not only converges and shares a similarly positive status, but also requires the idea of truth telling as a measure of respect, which is missing in the case of its main counterparts, namely the lie, fake or false. Also, the principles of "continuity", "predictability" and "legality" clearly conflict with what a crisis represents. The national security interests derive from the constitutional provisions and are related to "*legitimately* promoting and safeguarding" (Romania *National Defence Strategy*, 2015, p. 8) a series of core values. The *legitimacy*, which implies a system where authority is both claimed and accepted as proper for the society (Lipset, 1983, p. 64), is also important for the actual operational functionality of the main constraints within which truth is established. Not least, the national security objectives include, among other, the idea of "protecting the decision-making process against influences and/or illegitimate or non-transparent actions" (Romania Defence Strategy 2015, p. 9) – which is a direct reference to the typically sanctioned acts of manipulation, deception, espionage, blackmail, corruption etc. These all represent actions that imply different misuses of both truth and lie, and that affect the authority's ability to find or establish the relevant information, the actual "truths" it needs, and to autonomously act upon that base. In essence, it ensues there are uses of truth and lie that are officially accepted as convergent with the established set of values and principles, with the security interests and objectives, and others that are not tolerated. The latter category is so important that it is treated as a high matter of security and it receives the particular status of a "national security objective".

The German security policy is also presented as "tied to values and guided by interests" (Germany White Paper 2016, p. 24). Among the four (constitutional) values that are named, two are interesting – the *human dignity* and the *rule of law* – in the sense that they tie the federal policy first to an *axiological* content which is hardly favourable nor compatible to lies, fakes, false or even to the idea of crisis, and afterword to a more neutral *normative* content where truth may well be required or sanctioned, depending on specific legal conditions. Then, one of the main security interests is to "maintain the *rules-based* international *order*" (Germany White Paper 2016, p. 25), which amounts to a view of regulated world affairs, reinforced by the mention that the named order must be maintained "on the basis of international law". Furthermore, there are measures that Germany tries to embed in larger instances – namely, EU, NATO, bilateral/regional cooperation, and international law – and according to its conception of "security in the digital age" (German Cyber Security Strategy, 2016, p. 39) aim at enforcing specific requirements such as: the use of electronic *identification*, *signature*, *seal* and other *trust services*; the problem of *allocation/*

attribution of cyber-attacks and the necessary *exchanges of information*; the spread of *trust- and security-building measures*. All these represent basic practices that are essential for a minimal infrastructure for dealing with truth related issues: to know, to certify, to establish, to trust etc. And although they may not purposefully be intended to do so, they nevertheless contribute to such a system of knowledge and power. In this particular context, it becomes obvious that the strategic effort is not exclusively focused on the truth *per se* (identities, statements, information etc.), but it supports and aims at a more general *system of it* which must respond to requirements such as clarity, order and trust.

In both counties, there are actions that are officially considered as mishandlings of the truth – as they seem to affect its social status or contradict the already established uses of it – part of them being governed as risks and threats, as key security matters. These are not only affecting certain particular truths (from a simple information to more complex decision making processes), but have a wider negative impact on social values and principles, on security interests and objectives, on social arrangements and the order within which the respective truths are established. From this perspective, mishandlings and their agents affect what truth was agreed to be in that society, his common rules, instances and means. Then, not only the truth by itself (as a basic statement or the more general idea of it) represents a matter of security, but even more so the practices that revolve around it, how it is established and used, with which purposes, how it is distinguished from false etc. The security prism, with its "myopic and colonizing properties" (Goold, Loader, and Thumala, July 2013, p. 12), is not only interested on the truth *per se*, but on the wider *system of it*. In other words, the entire regime of truth is a matter of security, including the practices that it induces and that sustain it and the changes or crises that it suffers.

Being interested in all these nearby / collateral ideas and practices, related more to the power and knowledge dimensions of truth, the official documents move away from the well-known solemn oath regarding "the truth, the whole truth and nothing but the truth", towards an approach that concern a much wider and deeper social field. I appreciate that this extended field of official interest and agency could be very well named through a paraphrase: the truth and nothing but the whole system of it.

Under the signs of crisis and exceptionality – "the world is unsettled

Foucault warns that the regime of truth "is not merely ideological or superstructual" (Foucault 1980, p. 133), but the very "condition" of the formation and development of entire systems such as the capitalism, the

socialism etc. It therefore ensues that a crisis of the regime of truth – as a whole or through any of his core elements – represents a fundamental problem at the very crux of a system or a society and induces vulnerabilities, risks and threats, namely the precise constituents of a security matter. In this context, such a crisis also implies changes in the knowledge and power settings, through emerging actors (especially those who contest the established regime, are contemptuous of it or simply careless) and a series of discourses and practices that further influences its evolution, and finally the adjustment of the former systemic arrangement or the making of a new one.

The most obviously shared idea within the official documents under analysis is that the current security environment is, as the rest of the world, at the same time more threatening and difficult to understand, less visible and accessible for the instruments that contemporary actors use in order to access or establish the truth. The overall situation is characterized under the signs of crisis and exceptionality, especially from the power and knowledge points of view: power is shifting; profound changes; intricate security situation, complex, volatile, unforeseeable; unpredictable dynamics; uncertainty of intentions; blurred borders; deficits, declines and disintegration etc. While dangers seem to multiply, common perspectives, truths, even simple facts appear harder to agree upon. All this affect our capability to know and establish the threats, risks and vulnerabilities which represent key matters of security where an accurate truth acquisition (with at least as possible of its counterparts such as lies, fakes, false, disinformation etc.) is deemed to be vital for a society. In addition, the digital transformation contributes to a large-scale crisis phenomenon that affects the society as a whole, not just the cyber space, and the multitude and dynamic of changes makes the usual quest for truth more difficult and less successful.

The Romanian National Defence Strategy 2015-2019 begins by repeatedly acknowledging the "paradigm *changes*" (Romania Defence Strategy 2015, p. 3, 5, 6) of the national defence and security concept that are related to the "increasingly *unpredictable* dynamics" of an "*intricate*" security environment (Romania Defence Strategy 2015, p. 5). The current period of time is characterized as one where multiple risks, threats and vulnerabilities "*intersect* and *overlap*", acquiring "*new* dimensions", resulting in "*unforeseeable* effects" (Romania Defence Strategy 2015, p. 5) and "strategic *surprises*" (Romania Defence Strategy 2015, p. 6) at virtually all levels, national, regional and global. Changes, surprises and complexity, as well as the inability or impossibility to know, predict and foresee are all framed as part of a relatively *new* problem that is more specific for the *current* period of time. The document depicts our contemporary period as being, at the same time,

highly threatening and difficult to understand, risky and hidden, with threats that proliferate and vital truths (i.e. about dangers) that are harder to establish. One could also say that, not knowing (in)security's truths has negative consequences – causing and amplifying or at least exposing to risks, threats and vulnerabilities – and this seems to become the matter that dominates the strategic discourse.

Among the seven *threats* to the national security, two are of interest: first, the "increasing fundamentalist *propaganda*" that favours radicalization and extremist/terrorist actions (Romania Defense Strategy 2015, p. 15); secondly, the "hostile *informational* actions" that may affect projects and decisions at the state's level (Romania Defence Strategy 2015, p. 15). Both imply practices that are considered contrary to the accepted types of discourse or that threaten the established status of those in charge with state decisions. Three other threats are voiced in terms of "instability" and "distortions" that alter Romania's security (Romania Defence Strategy 2015, p. 15), which reinforces the conservative stance and the negative strategic discourse on crisis and change. The same type of discourse is adopted for the presentation of the main *risks*, pointing towards the negative security consequences of different "instabilities", "trends" or "distortions" (Romania Defence Strategy 2015, p. 15). In addition, a number of *vulnerabilities* are held responsible for limiting the state's "ability to assess" (Romania Defence Strategy 2015, p. 16) the threats and risks. Evidently, this is not about the truth itself, but it represents a related or nearby problem because it affects the state's grip on the information that it needs about the threats and risks, and these information must reflect the truth as accurately and completely as possible. If not, the document sees a security problem, namely vulnerability.

"The world is unsettled" – the crisis-aware mood of the White Paper on German Security Policy is established from the very first words of the opening remarks by the federal chancellor, Angela Merkel (Germany White Paper 2016, p. 6). This precarious state of a "changed security situation" is something that one can "see and feel" through the impact of "crisis and conflicts" tending to replace "peace and stability" in ways that "would not have believed it possible". These are very strong affirmations, first by their appeal to the very basic senses when referring to the current crisis, secondly by openly admitting a state of strategic incredulity when considering the consequences of the crisis. The German security environment is further described as "complex, volatile and dynamic" and therefore "unpredictable" (Germany White Paper 2016, p. 28), each of these attributes portraying a problematic milieu for knowledge practices that are intimately related to the seeking of truth. In addition, the repetitive use of degree adverbs like *more* or *increasingly*, clearly frames a trend within the security

environment that, without necessarily amounting to a crisis, raises a number of challenges. The international, also decrypted as an "order in transition", is undergoing "profound changes" that are said to be driven by the increasing interconnectivity of our world. First of all, this brings "better access to information" (Germany White Paper 2016, p. 28) for more people, which potentially equals with better prospects for searching and finding the truths each one may be looking for. Secondly, it also results in "interconnection and spread of risks as well as their repercussions", among which are explicitly indicated the "information operations" – a specialized practice that revolves around information as an element of power, not aiming at truth or lie, but using them as means to power related ends. Hereabouts, the document widely opens towards the idea that specific misuses of truth, such as the information operations, are risky, repercussions and simply inacceptable for the security of a society.

The White Paper treats these changes as part of a more general crisis of the current order, under the pressure of different drivers, such as "deficits" in identity and legitimacy, "declines" in norms and values, "disintegration" of state centred orders (Germany White Paper 2016, p. 29). This image of a 3D challenged social order (deficit, decline, disintegration) does not offer a favourable background for any type of systemic arrangement, for stable and undisputed regimes. On the contrary, it may represent one of the reasons for the widely perceived crisis of many power and knowledge settings. For example the state, one of the main modern social and political constructions, that is here qualified as "the central element of order" (Germany White Paper 2016, p. 29), appear to be challenged in many parts of the world, in ways that are contributing to conflicts and crises. The strategic narrative could not have been clearer in this instance – challenges to order affect security! – and imply a logical choice in security matters: *order* is preferable to *crisis*!

In order to cope with such a milieu, the White Paper underlines the need of being "fully *aware*" of it, a prescription that blends the seeking of knowledge/truth with an ambitious monitoring discipline. It's also worth noting that this prescription adopts the imperative tone of an ultimative warning – "*only* by being *fully* aware…" (Germany White Paper 2016, p. 29) – and frames itself as a comprehensive sine qua non condition. In other words, without a fully-fledged awareness, security is not possible. Not knowing some emerging risk trend, not being aware of a remote challenge would then represent an exceptional security matter and would severely hinder the entire security policy, from its ability to "target the causes" to the capacity to "anticipate future developments". Fuelled by this accentuated awareness, the White Paper also formulates many political prescriptions that are intended to address this state of unsettlement and insecurity, the most relevant being an

absolute rejection of *crisis* ("at all times, our aim should be to prevent crises and conflicts"), a stronger devotion to *order* ("greater commitment to security, peace and a rules-based order") and a focus on *resilience* ("throughout government and society") (Germany White Paper 2016, p. 29).

In a world where "power is changing - power is shifting" (Germany White Paper 2016, p. 30), the White Paper tries to prepare the German security for a new and dangerous global order that risk to "weaken the universally binding nature of the foundations and institutions of our current global order" (Germany White Paper 2016, p. 31). The strategic stance is clearly opposed to the weakening of the core elements of the current order, which is framed as a threatening trend that must be countered. There is a concrete situation that is explicitly treated within this frame: the "rules-based Euro-Atlantic order of peace and stability" (Germany White Paper 2016, p. 31) called into question by Russia, by using hybrid approaches that "purposefully blur the borders between war and peace" and by creating "uncertainty about the nature of its intentions" (Germany White Paper 2016, p. 32). At this point, the main problems are truth related: "blurring the borders" makes truths harder to distinguish, while the "uncertainty of intentions" has a similar effect and also reduces trust. Therefore, for a solution, what appear to be important from a security standpoint is the "consistent adherence to existing and proven common rules and principles" (Germany White Paper 2016, p. 32) – in a nutshell, proven rules are essential to security.

The strategies analyzed are deeply rooted in- and animated by the idea of a profound crisis of our current knowledge capabilities, of our emprise on the truths of the security environment. The official documents suggest different crisis dimensions and their respective consequences, and each time these are framed as matters of security, mainly because they are perceived as sources of insecurity. The narrative of an "unsettled world" illustrates an synthesizes very well the crisis-aware mood of these security strategies, their inner *Zeitgeist*, and offer the image of a deeply challenged social order, affected by fundamental changes in all areas, from ethical to technological, from individuals to states, from acceptable discourses to truth handling practices. There is here something of the typical process described by the securitization literature (Buzan et al. 1998), that way of presenting a particular milieu or the entire world by pointing to vital dangers and challenges, and then to the exceptional means that need to be enacted in order to deal with them. And it worth observing that this is the case with all documents analysed, which means that the highest official discourse contributes to a general securitization process of virtually all the major "lectures" concerning the world we currently live in. This observation

confirms and complements other findings about a multiplication of the actors who feed the public fears and enable security to "trump" other considerations and values (Zedner, 2009).

Despite some minor and rather rhetorical openings towards what a crisis may imply in terms of opportunities, the strategic stance is very clear and eager to show that challenges to order affect security and that *order* is systematically preferred to *crisis*, from a security perspective. All these documents operate with an absolute rejection of crisis, which is treated as a danger (the very basic security matter), including by a plethora of prescriptions that are meant to address it like a threat. Even the security's "normalcy" and the corresponding ideal securitizing moves are framed in terms that essentially imply to prevent or overcome any kind of crisis, obviously including the one surrounding the handling of truth. One could say that, given the special place and status of the crisis as a danger construct, security documents embrace a *crisophobic ideal*, which – in a paradoxal way – transforms any crisis, actual or potential, into a matter of security, into something to secure.

Therefore, not only different particular truths and the rules that surround their social uses are treated as matters of security, but even the crises that current regimes of truth are facing. All these official documents indicate in an indirect but rich manner the increased dilution or irrelevance of traditional milestones and truth establishing practices, the shrinking of our capability to separate truth from false in key security problems, the rather *ad hoc* and exploratory search of means intended for sanctioning each other, the uncertainties around who and how could decide what counts as truth when security is at stake, the need for new techniques and procedures to be adopted for securely handling the truth etc. These problems and many other punctual issues not only contribute to the general *perception* of a crisis, but are also indicative of *how* the crisis itself becomes a matter of security: beyond the already discussed crisophobic official stance of security, we also notice a gradual overlapping of the symptoms of the crisis affecting different elements of the regime of truth over key themes of security. As a danger construct, the crisis of truth related problems is thus connected to a series of securing ideas and acts that makes it a typical security matter, as defined in my theoretical perspective.

Establishing truth within a virtual space – the cyber

Despite its virtuality, the cyber is officially understood and presented as the forestage, the *proscenium* of more fundamental social changes and

crisis, as a truly dangerous space. It is considered to be the scene of real threats that can also have an impact in other physical or social spaces, and its characteristics raise challenges to some of the most usual truth establishing practices of a state. This particular status comes especially from the fact that, in the cyber space, it appears to be even more difficult to establish or sanction truth and its counterparts, which represents a major social preoccupation and, as we have already seen, also a matter of security.

The Romanian Cyber Security Strategy 2013 underlies the major impact that the modern technologies had on the entire society, resulting in "true mutations" within its inner "functioning philosophy" (Romania Cyber Strategy 2013, p. 4) in all major social areas, as well as in the daily life of the individuals. The use of the term mutation here is very interesting, especially as its primary use in biology refers to permanent changes in the sequence of an organism's DNA. In this context, the reference to "true" seems to play more as an emphasis for the fundamental character of the changes that the society is undergoing, a paraphrase for crisis within the very core of the modern social, a crisis through which the technology becomes a central premise or an even ontological part of what contemporary society is, of its social DNA.

The cyber space is defined as a "virtual" milieu (Romania Cyber Strategy 2013, p. 7) – therefore not exactly real, but rather a computer generated or simulated one – that includes both the informational content and the users' actions. Despite the *virtual* nature, the cyber, just as other security environments, is framed as a *dangerous* space, with consequences that trespass its bodiless borders into the *real* physical or social spaces. Many countries have experienced cyber-attacks and even preparing for "conflict in the virtual dimension" (Reveron, 2012, p. 4). Therefore, (in)security is understood as an ubiquitous issue, beyond virtual or real spaces. Within the cyber-space it is very difficult to establish or sanction truth and its counterparts, which causes a plethora of anxieties. Moreover, its gradual expansion would "introduce vulnerabilities" (Romania Cyber Strategy 2013, p. 4) in the society and it is then framed as a special issue that "must" be treated as a "major preoccupation" by all actors involved – a typical securitization approach. The combined deduction of the two ideas is that a milieu where minimal truth requirements (identities, statuses etc.) cannot be established represents a security problem, both as source of dangers (risks and vulnerabilities) and as a challenge for the acting system of power.

This new and threatening cyber appear as a space that must be secured and the strategy aims at a "*safe* virtual milieu" that should be highly "resilient and trustful" (Romania Cyber Strategy 2013, p. 6). Beyond the fact that the concept of resilience has been imported in many security and

governance challenges (Aradau, 2014, pp. 73-87), it is interesting to observe how security is based on characteristics that are also important for the functioning of a regime of truth, namely its ability to withstand punctual attacks / contestations or a more general crisis (resilience), as well as an underlying confidence or acceptance of its main actors, speeches and practices (trust). Security and regime of truth appear to share a number of common conditions.

In a similar vein, the Cyber Security Strategy for Germany 2016 underlines right from the introduction the accelerated and profound social changes that are brought by digital transformation, which "radically changed Germany in just a few years" (Germany Cyber Security 2016, p. 4). *Change* is the key-word and it describes processes that characterize not only the cyber space, but the society as a whole, indicating a large-scale crisis phenomenon, in its general and etymological Greek sense of a time with risks and opportunities, when important decisions must be made. In this context, it is the state who "has the duty to assess and act" upon these processes of change, as the most prominent actor, alongside with industry and other stakeholders. Because of the acute perception of a crisis situation and of the risks it implies, two correlated issues are raised, first the need for "trust" and "confidence", and secondly the status of security as "an essential aspect" (Germany Cyber Security 2016, p. 4). This implies that overcoming the crisis would not be possible without a viable nexus of *trust* and *security*, both being mainly in the responsibility of the State.

Further concerns are related to the diversity and status of the attackers (states, groups or individuals, often with "criminal, extremist/terrorist, military or intelligence background") and the methods for concealing that "complicate detection, mapping, defence and prosecution". It is, basically, the problem of perpetrators hiding the truth and defenders not knowing and/or being able to establish the truth about who-did-what and whom-to-punish – which raises an "especially large risk of uncontrolled escalation", a serious security matter. This challenges to the usual truth establishing ambitions of a state, namely the classical police questions of *who* to identify as perpetrators*, what* they do, and *how* to deal with them – and answering these questions is essential for the functioning of a security apparatus.

At the end it becomes obvious that – from an official perspective – the virtual cyber-space is not only the *forestage*, the *proscenium* of changes that technology brings into the modern societies and which allows the state (and also other social actors) to make predictions and plans, to access or even produce future truths ahead of time. The cyber is also the *entire arena* where spectators and actors, citizens and/or users can see (and interact with) a state trying to

replay the historical piece of establishing typical governmentality mechanisms over a new space and its social relations. The cyber in its entirety, including rules for handling the truth, appear as a socially and technologically emerging construct.

An official and axiomatic system for the knowledge-security nexus

The problem of the correlation between *knowledge* and *security* is a matter that dominates the strategic discourse and is visible in each of the official documents under analysis. While references to *knowledge* may appear as a partial link to the truth itself, in fact they include most of the wider truth related issues that are of interest from a security standpoint, namely its acquisition, its separation from false, a set of particular skills in approaching and dealing with truth and its counterparts. Taken together and synthesized, these various references form an almost axiomatic system of ideas and statements that are treated as self-evident or necessary truths. The first axiomatic idea that knowing the (truth about) dangers improves the security odds as it offers the basic conditions for some of its very important practices and / or statuses such as anticipation, prevention, signalization, predictability, and understanding. *Reciprocally*, not being able to establish the truth about dangers means less security as it amplifies vulnerability or, with the exact words employed by the documents, it translates in unpredictable dynamics, unforeseeable effects, strategic surprises, or lack of understanding. *Complementarily*, the distortions and counterparts of truth generate insecurity in multiple forms: instability; hostile propaganda and informational actions; vulnerable decision-making process; influences and/or illegitimate or non-transparent actions etc.

Against the fallible epistemological background of an unpredictable and difficult to understand security milieu, in order to manage a large array of issues considered to be "vital", the Romanian National Defence Strategy points towards the need for "*knowledge* of evolutions in the security environment" (Romania Defence Strategy 2015, p. 6) which is treated as being "of paramount importance" (Romania Defence Strategy 2015, p. 11). Knowledge is here understood as a *recognition* of something that exists and manifests in the world, as a *narrative* or a *tale* of the world that "tracks the truth" (Nozick's influential "tracking theory" of knowledge) (Nozick, 1981, pp. 167-196) and that should not be affected by the counterparts of truth, being "neither fictions nor opposed to facts", although "always inmmersed in history and never innocent" (Escobar, 1995, p. 19-20). Such a narrative is bound 1) to correspond to evolutions in the environment (i.e. a correspondence approach

of truth) and also 2) to be of interest from a security perspective (i.e. to concern risks, threats or vulnerabilities). These two validity conditions, of truth and relevance, describe very well a kind of "situated knowledge" (Haraway, 1988, pp. 575–599), one that is specific and corresponds to certain situations. The security strategies do not aim at a purely scientific knowledge even if research may punctually be involved, but at this type of situational knowledge that is expected to be both true and actionable, which indicate a rather pragmatic approach. At what Foucault calls a "preconceptual level" (Foucault 2002, p. 68), security documents cannot make an appropriate use of the idea of knowledge, more precisely of the "need for knowledge" without first implying a relation of dependence of knowledge to truth. In the absence of truth, knowledge cannot define a domain of validity for itself within the security field, as maybe in any other field. This is why, without bothering with too complex epistemic or philosophical considerations about the relation between knowledge and truth, the official documents embrace the naïve realism of a knowledge that simply has to track/represent the truth about security matters of interests, to be able to separate it from fake, false or misleading. They signal that truth is an essential condition of the knowledge they praise, which is not explicitly stated, but also not less important for that reason. Truth is not confounded with knowledge. Nevertheless it represents, in this context, its most basic requirement, a constitutive criteria in the absence of which one could not speak of *knowledge* or at least that would not respond to the *need* praised by security documents.

This need for knowledge also induces the reciprocal idea, namely that not knowing certain evolutions in the environment hampers the ability to "responsibly manage" their impact, thus affecting the security of the country. The strategic prescriptions given by the lines of action add a new emphasis on "*knowing* the risks and threats *in all aspects*" (Romania Defence Strategy 2015, p. 18), on "*understanding* the nature of threats" through scientific research (Romania Defence Strategy 2015, p. 21). Moreover, the lines of action established for the intelligence, counterintelligence and security dimension are of special interest through their bold emphasis on one hand on "*knowing*" and "*identifying*" different threats, and on the other hand on "*signalling*" and "*drawing attention*" to the established beneficiaries (Romania Defence Strategy 2015, p. 19-20). In essence, this describes the functions and priorities of a systemic arrangement for seeking, establishing and circulating the knowledge regarding security matters, while also bespeaking its fundamental character.

Moreover, the broadening of the "*anticipation* capacity" is considered nothing less than "fundamental" and the development of systems for the

"early spotting of dangers" is qualified as "mandatory" (Romania Defence Strategy 2015, p. 18). Again, the main idea is that (early) knowledge and the related capacity to establish truth preserves a larger room for action on social situations that have not (yet) developed into real crises or conflicts. A strong assumption is made, namely that a well informed and opportune action on a truly dangerous situation will prevent it to become true. It is a positively valued so called "self-denying prophecy", a special kind of knowledge that – when coupled with the right action – would falsify itself by changing the social realities. This assumption emerges quite often within the security professional culture and it is quite relevant for the regime of truth because it means that it is good to bend the-now-true-course towards a threatening reality, by acting on key conditions in order to falsify that course and prevent him to become true. It means that – for security purposes, for order or stability – one can and should falsify a (potential) truth and replace it with another, more suitable, social reality.

In order to resume, knowledge and the related capacity to establish truth about threats and their perpetrators offer more options, time and space for security oriented action. Not knowing (in)security's truths has negative consequences, causing, amplifying or at least exposing to risks, threats and vulnerabilities. It worth noting the dramatically staging and justification of the need for knowledge (paramount, vital, mandatory, fundamental, in all aspects etc.), which are further enhanced by a very contrasting accent on the current problems and limitations (unknowns, intricacies, complexity, unpredictability, uncertainty etc.). The actual content and also the tone of these texts express a sense of inadequacy between means and challenges, a state of crisis for our knowledge capabilities that would not be up to security needs and requirements, and thus would not allow for an adequate "tracking" of truths related to key matters of security. When the latter happens, resilience understood as preparedness for crisis and being able to cope (Omand, 2010, p. 57 and 63) appears to be the last resort/hope for the strategic narrative: who is unable to know or to establish the truth should, at least, be able to resist and to manage the consequences. For the strategies and programs analyzed, these principles appear to have enough consistency and coherence, practical relevance and general applicability, and they are so thoroughly used that they became an official and axiomatic system of thought about the knowledge-security nexus.

Specific elements of national narratives

The research question has also a comparative dimension, with focus on the meta-narratives that are produced in relation to the core elements of

the regime of truth in the respective German and Romanian security contexts. Tellingly, while most of these are commonly shared by the two societies, there are also aspects that are specific to their respective German or Romanian security context, and that are not consistently reflected within the documents of the other country. These differentiations seem to be rather local nuances and do not indicate a strong contrast in the approach of truth, but are nevertheless important for the comparative perspective of this research.

The Romanian specificity is given by the worries and prescriptions surrounding a two folded idea, focused on unity and status. Firstly, they regard the inner *unity* that must be achieved through "national *cohesion* and *consensus*" (Romania Defence Strategy 2015, p. 6). Moreover, one of the main principles for this process is the coordination through unitary conception and plans. The strategy formulates hitherto a statement that not only matches the classical coherence approach of truth, but (more important for the theoretical perspective of this research) also sets the *national* arena as the main framework in which the Romanian security apparatus deals with the truths that it seeks/produces/ manages, and gives a certain political dimension to the process. Secondly, there is a solid concern for the symbolic *status* within the world, which results quite clearly from the will to strengthen the "strategic *credibility*" based on "*continuity* and *predictability*" (Romania Defence Strategy 2015, p. 6) as well as from the cautious legitimating of the nature and performativity of the national security interests (Romania Defence Strategy 2015, p. 8).

The German particular approach is based on two elements, namely rules and a strong emphasis on collaborative approaches. Firstly, out of security interest, Germany is on the pursuit of a specific type of order (Germany White Paper 2016, p. 52), an order that is based on *rules* (norms, values) rather than on other regulatory elements such as the known Smithian invisible hand, historicist determinism, religious visions etc., and that is clearly pro-regime and anti-crisis. It explicitly states "right, not might!"(Germany White Paper 2016, p. 53). Secondly, security related truths are better found/established within structured arrangements, in *cooperation* with other relevant actors and according to specific rules and procedures, in "integrated networks of actors and instruments" (Germany White Paper 2016, p. 15), among "reliable and dependable partners" (Germany White Paper 2016, p. 8) that "embrace mutual interdependence" (Germany White Paper 2016, p. 23) and combine their expertise to "create a clear overall picture" (Germany White Paper 2016, p. 50) – a systemic arrangement that even implies a "cross-generational responsibility" and, obviously, tends to embrace the coherence declination of truth. This also gives a certain political dimension to the process and establishes the *European and international* arena as the main

framework wherein the German security apparatus deals with the truths that it seeks, produces or manages – but still observing "a clear national position" (Germany White Paper 2016, p. 25). Overall, a key supposition became obvious, even if not directly stated, namely that shared security implies a minimal common framework of truth and trust, as a necessary condition and basic infrastructure for enhanced security cooperation. The same approach is adopted for the governing of the cyber space, through measures that facilitate cooperation, exchanges and inclusion: government and business must "work closely together" at all levels and have a "trustful" and "intensive" exchange of information, surpass the IT skills shortage through "networks of specialists" and "personnel exchange programs" (Germany Cyber Security 2016, p. 21). For the German strategists, security is a "whole of society endeavour" (Germany White Paper 2016, p. 58), just as a (the?) grand and coherent social truth.

An official Faustian pact – truth as a mean towards security

The official security discourse of these documents addresses a long list of problems – old phenomenon and new changes, known and even unknown threats – and for some of them it requires extraordinary measures beyond politics as usual. The way in which the official documents approach truth related issues and critical situations that affect its "normal" uses is indicative of a perceived crisis of the regime of truth. And this is a problem that concerns my research: why and how unfolds this framing of truth and its counterparts in relation with dangers – risks, threats and vulnerabilities – rather than with ideas such as opportunity, positive social changes or some new philosophical basis for the understanding of truth. According to the narratives analyzed, the securitization of truth, of its regime and crisis, does not appear as the exclusive result of new and successful speech acts coming from official actors within the society. It seems that it is based rather on an already solid understanding of the status of truth as a mean (among other) towards security as end. The texts made it clear that security has a higher strategic and official status and, as such, one can or even should transact truth in order to achieve and preserve security, especially in an increasingly dangerous environment.

This is the very motif of an official Faustian pact through which authorities set the conditions for a bargain whereby public and private actors should sacrifice something of spiritual or moral importance (*truth* in this case, but also *liberty* and other in different instances) in order to obtain social or individual benefits (*security*). These conditions are not structured as a proposal about which the different actors involved could autonomously decide, but rather as imperative lines of behaviour where the main truth

handling practices are already established, officially leaving small merges for option. The key (im)balance of truth and security is nowhere in these documents allowed to come into question, and this is how the regime of truth endeavours to prevent even the eventuality of a questioning of the structural options that subordinate the handling of truth related practices (access, dissemination, classification, en-/decryption, warning etc.) to aims of security. In this perspective, truth appears as a central social and cultural value that finds its official limits not in other supposedly immuable values, but rather in security motivated concerns and objectives, in a specific conception of security as "normalcy", in the official will and emprise over *what* and *how* gets to be established as relevant or true, or in that axiomatic understanding of the knowledge-security nexus.

Nevertheless, it is difficult to identify what exactly is truth for the official strategists. There is no direct and explicit statement within these documents and one plausible cause could simply be the fact that there is no interest for the inner nature of truth, but rather for the nearby practices that concern its establishment and acceptable uses, for its regime. While the word "truth" does not appear as such in any of the studied documents, there are strategic statements that concern how truths should be treated as means of security, which are the good and acceptable ways to handle them or, the opposite, the bad and dangerous ones. Moreover, the official security strategies do not share a unanimously positive perception of truth. On the contrary, truth is far from being treated as an immuable value, subtle but numerous distinctions being made among different categories such as useful or irrelevant truths, to classify or to disseminate, to elicit or to protect etc. The official status of truth is measured by how it fits with the needs, ideas and rules of the respective society, mainly of the state, and priority is given to those that are considered to represent matters of security. This is one of the main avenues by which security matters (as exceptional political problems), practices and ways of thought contribute to the construction / establishment of a regime of truth.

If I should still try to answer the question of "what is truth?" from the strategic official perspective, I would mostly have to point that, essentially, truth is what security – discretely – makes of it, without any further complex definition. For the strategic official approach this seems to be enough and it unveils a certain will of power/security over truth that is obvious each time truth becomes, through its regime, a mean towards another end, usually expressed in terms of security.

This way of approaching the matter speaks also about the barely visible disciplinary technologies of power and punishing mechanisms that are

supposedly directed towards some marginal "others", those who mishandle the truth, and not against the "responsible" citizens and society who observe and act and behave according to the established rules. These documents reflect and contribute to technologies of power that are centred on a *state* that is still seen as an anchor for the social order, on the generally good but endangered *citizen*, and also on the figure of a so-constructed *mishandler* of truth, a human or social actor that breach the established procedures and periclitate the "normal" order. Such a discrete but consistent securitization of the regime of truth unveils itself as an instrument of disciplinary power that is employed as a governmentality tool by the officials, politicians and security professionals. It is worth noting that within this official perspective of security understood as normalcy, to securitize a regime of truth implies the claim to normalize its state against different challenges and abnormalities that may affect his core elements or to overcome the crisis that hampers its normal functioning; in short to claim exceptional means in order to impose the norm(al) and to discourage or punish deviations.

My initial approach of such documents as objects of study did embrace a played naïveté, one that was meant to allow now to ask in a typical Foucauldian way: why the presence of such a key issue as the problem of truth within modern security documents has not been observed earlier? These strategies cannot offer a complete answer to such a question. Nevertheless, they clearly indicate that within the security milieu one can find a very consistent *interest*, a complex *understanding*, and a multitude of concrete *practices* that focus on the social uses and creation of truth. And yet, those who produced the documents did not explicitly refer to truth as a concept or as a general idea, and only implicitly addressed the main elements of its regime. Although the word "truth" is nowhere mentioned in these texts, the authors repeatedly and consistently focused rather on issues and series such as: knowledge, understanding and their limits; different distortions, manipulations, influence and propaganda practices; espionage, covert operations, subversion and other informational actions; concealment, anonymity, classification, encryption; blurred boundaries, obscured roles, hybrid threats, undetected attacks, strategic surprises; awareness, monitorization, dissemination, early warning; order, rules, normalcy; crisis, disintegration, carelessness etc. All of these belong to a wider framing of truth and they represent small units that, through series and relations, reconstitute a barely visible puzzle.

In this context, in order to try an answer to the upper question, I emphasize that this puzzled problematization of small and disparate elements, the focus on details and the use of argotic terms contribute to obscuring a deep and wide approach of the problem of truth as a matter of security – even for

those who are close or activate in the field. Furthermore, the strong perception of security as the *central* or *end* subject of these situations and actions does not help to see in the different truth related elements something more or au delá of the usual and already familiar "security issues". This security prism or perspective is increasingly popular and used not only by security professional actors, such as the police, the military or the intelligence institutions, but also by politicians, business and corporations, mass media and the general public opinion. As Buzan, Waever and Wilde (1998) have indicated with their widening of the security agenda, we tend to speak security in many sectors of the social life, from military to political, societal, economic and environmental – and by specific processes of securitization the issues are reframed, which produces new understandings and problematizations, sometimes focused more on security aims, procedures and acts, than on the initial/basic issue. This means that when a referent object such as an element of a regime of truth is securitized, one still sees the security stakes and processes, rather than their truth related object.

What still remains to be understood is whether this deeply fragmented and nontransparent framing of truth within the security official discourse is the purposeful result of a conscious conduct, or something that simply emerges from the current professional routines and frames of thought. Regardless of the answer, with or without intentionality, their micro frames and handlings of different truth related elements contribute to the wider social and political regime of truth, having a certain constitutive effect. And this is precisely what Foucault was referring to when he indicated that documents also produce the very actors that use them (Foucault, 1991, pp. 87-104).

These official documents contain an impressive body of statements and practices that concern the dynamics by which truth related issues are addressed (understood, framed and managed) through security ideas and processes – namely the exact research problem I raised. They indicate the acceptable security discourses, what should be considered truth and what cannot, but also how the truths are to be handled by different subjects through specific practices, sometimes stating the respective consequences in case of misconduct. The strategies even establish and define specific spaces/milieus such as the cyber, the privacy, the national, the international, wherein such statements and practices can be enforced, promoted or newly created – thus playing a double role, discursive and actional, at the same time.

To resume, the official security strategies see, understand and address the issue of truth in an indirect manner, with a tendency to impose an etatist frame of mind, justifying the state's views as the acceptable narratives, mainly for reasons related to security and authority. This contributes to giving the

authority of "truth" to an official speak that, through specific practices and frames of thought, creates the truth as a matter of security and claims the authority to regulate its regime.

References:

1. Aradau, Claudia, (2014), "The promise of security: resilience, surprise and epistemic politics" in *Resilience*.
2. Buzan, Barry, Waever, Ole, Wilde, Jaap de, (1998), *Security: A New Framework for Analysis Boulder*, Colo.: Lynne Rienner Pub.
3. *Cyber Security Strategy for Germany*. Berlin: Federal Government, 2016.
4. Escobar, Arturo, (1995), *Encountering Development: The Making and Unmaking of the Third World*, Princeton: Princeton University Press.
5. Foucault, Michel, (1991), "Governmentality" in *The Foucault Effect: Studies in Governmentality*, London: Harvester Wheatsheaf.
6. Foucault, Michel, (2002), *Archaeology of Knowledge*, London: Routledge.
7. Foucault, Michel, Gordon, Colin, (1980), *Power/knowledge: selected interviews and other writings, 1972-1977*, New York: Pantheon Books.
8. Goold, Benjamin, Loader, Ian, Thumala, Angelica, (July, 2013), "The Banality of Security. The Curious Case of Surveillance Cameras" in *British Journal of Criminology*.
9. Haraway, Donna, (1988), "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective" in *Feminist Studies* Vol. 14, No. 3, pp. 575–599.
10. Hodder, Ian, (2012), "The Interpretation of Documents and Material Culture" in *Sage Biographical Research*. Ed. John Goodwin, Thousand Oaks, CA: SAGE Publications, Inc.
11. Lipset, Seymour Martin, (1983), *Political Man: The Social Bases of Politics* (London: Heinemann), 2nd ed.
12. Navaro, Yael, (2007), "Make-believe papers, legal forms and the counterfeit: Affective interactions between documents and people in Britain and Cyprus" in *Anthropological Theory* 7: 79.
13. Nozick, Robert, (1981), *Philosophical Explanations*, Cambridge, MA The Belknap Press of Harvard University Press.
14. Omand, David, (2010), *Securing the State*, London, Hurst&Company, 2010.
15. Reveron, Derek S., (2012), *Cyberspace and National Security: Threats, Opportunities, and Power in a virtual world*, Georgetown University Press Reveron 2012.
16. *The Romanian Cyber Security Strategy 2013*. Bucharest: Government.
17. *The National Defense Strategy 2015-2019*. *"A Strong Romania within Europe and the World*. Bucharest: Presidential Administration, 2015.

18. Weber, Max, (1968), *Economy and Society: An Outline of Interpretive Sociology* (New York: Bedminster Press), 1968.
19. Zedner, Lucia, 2009, *Security*, Routledge.
20. *White Paper "On German Security Policy and the Future of the Bundeswehr"*, Berlin: Federal Government, 2016.