AARMS Vol. 18, No. 1 (2019) 59–77.

DOI: 10.32565/aarms.2019.1.4

The U.S. Response to the 2016 Russian Election Meddling and the Evolving National Strategic Thought in Cyberspace

(Part 2)[1]

Dóra DÉVAI[2]

Given the technical, societal and international nature of cyberspace, national cybersecurity strategy formation demands a hybrid approach of homeland security and the more traditional national security processes. Moreover, as the series of the latest publicly known cyber incidents against the U.S.—the 2014 OMB espionage, the 2015 attack against Sony Pictures, the 2016 DNY attack or the Russian election hack and leaks—show, the dilemma of a proportionate response is a thorny technical, political and strategic task, while the need for a strategic level response is ever growing. Based on the analytical framework elaborated in the first part of this study series, the second part gives a strategic insight into the major determinants of the national response policy options to substantial cyberattacks against the U.S. The article also discusses wider strategic features pertaining to cyberspace, including strategic value of cyber weapons, threat perception, and national strategy cultures, which fundamentally impact cybersecurity and strategy formation.

Keywords: *U.S. cybersecurity policy, strategic culture, influence operations, cyber deterrence*

Major Technical, Operational and Strategic Considerations

In the U.S., responding to cyberattacks of substantial effects more actively and in a sustainable manner have been called for since the mid-2000s. Both policy and private sector communities have been demanding a national security level response instead of a cyber "Maginot-Line" style cyber defence comprising conventional software patches, intrusion detection and fire walls, or pure reactive cyber defence following incident management approach. The DoD introduced the idea of *active defence* in its 2011 strategy. Up till now,

[1] This is the second part of a series of three articles. The third part of the article continues the discussion with a concise overview of the Russian strategic context of influence operations.

[2] Ph.D. student, National University of Public Service, Doctoral School of Military Engineering; Devai.Dora@uni-nke.hu; ORCID ID: 0000-0003-1024-4474

however, active defence is still a very fluid concept running from situational awareness through deception to power projection and offensive cyber operations in cyberspace.

For quite a while, at the level of state-to-state relations, naming and shaming, a low-key instrument used to be the only explicit official reprisal applied by the administration. It was only after the Sony incident in late 2014 that a firm bipartisan consensus evolved that similar attacks cannot remain unanswered. In 2016, the White House's official reaction was criticized as too little and too late, but it did manifest a shift in official response. The next section will discuss those aspects that come into play when a response is considered thoughtfully.

Deterrence in Cyberspace

The need for a more strategic approach to cybersecurity first arose mainly in the academic and military expert circles. As opposed to the case-by-case, ad hoc crisis management, strategic thinking is anticipatory and pro-active, and synthetizes national interests and objectives. By 2008, as the opening citation in this article shows, President Obama's national security team realized the demand for a new policy and intended to meet it, though its attempts were often frustrated by Republican lawmakers and powerful commercial lobby interests in Congress. For the moment, the U.S. Government's official stance is that each response to a significant cyberattack will be examined on a case-by-case basis and it will combine the most suitable elements of national power. In Obama's words, we will respond at a "time and manner of our choosing". Still, the intention is broader than just neutralizing a given attack, and aims to contribute to deterring future attacks, as well. In generic terms, a cybersecurity strategy first and foremost seeks to avert substantial cyberattacks—or strategic effects caused by a cyberattack—by threat actors in a manner that is synergic with the overarching national security or grand strategy framework. The question of "how" *(ways)* is still an unsettled task. Deterrence is just one of several possible strategic concepts, along with alliances, reassurance, diplomacy and norm promotion, dissuasion, economic rewards and punishments.

Deterrence dominated Western strategic thought in the kinetic realm during the Cold War. Strategic nuclear and conventional military deterrence was considered a major tool to prevent large-scale kinetic attacks and maintain international peace and stability. Nevertheless, theoreticians have been arguing for long that this view focusing only on military threats and means to counter them is too restrictive. The feasibility of cyber deterrence is still contentious in many aspects. Cyber intrusions are extremely difficult to detect, and any computer system is inherently vulnerable. The attribution of the attack and the brandishing cyber offensive capabilities are problematic. Hence, the Cold War era model of deterrence was soon discarded as infeasible in cyberspace. [1]

Deterrence theory persists as the departure for cyber deterrence discussions. It consists of some basic principles: "…in order for deterrence to succeed, a deterrer should have sufficient capability, its threat should be credible. It is the adversary's perception and decision making that has to be affected: the cost-benefit calculations inherent in instrumental rationality are assumed to be present in decision situations involving deterrence. Deterrence is achieved if and when a potential attacker, fearing unacceptable punishment or denial of victory, decides to forgo a planned offensive. […] Most specialists have recognized at least two distinct

paths to deterrence: punishment or cost-imposition, and denial. The threat to impose costs in retaliation for a transgression obviously involves a negative incentive. But deterrence by denial also rests upon a form of negative incentive. The ability to resist and ultimately frustrate another actor's efforts can deny it any benefit while still leaving it with the costs of its efforts, again leading to a net negative outcome for the other side. A pure defense posture also does not aim to influence the other's decision; it accepts that an attack may occur and aims only to ensure the attack will not succeed." [2: 2, 38]

There is a tendency among the political elite, the Congress and the executive branch to treat deterrence in cyberspace as an umbrella term for all kinds of cybersecurity strategic ways. Conversely, it is still a question what role deterrence can play in cybersecurity, and what kind of deterrence strategy is the most feasible. In any case, one baseline step has crystalized that cyber deterrence needs to be broad or comprehensive. If deterrence is regarded as a strategic end in itself, then offence, defence and resilience are the ways to achieve it, through whole-of-government means (military, diplomacy, law-enforcement, resiliency, etc.). Deterrence by denial is gradually gaining more acceptance in cybersecurity strategies. It encompasses all forms of IT security measures, as well as any methods to improve resilience. Resilience is an elusive concept, but in general terms it means that once systems were knocked out, there are either redundant devices, and/or procedures in place to have them bounce back as quickly as possible. Cyber defence is no less elusive, as attack capabilities are developing at a neck-braking pace and it is almost impossible to keep up with. Cost-benefit calculations are always crucial in strategic planning, and given that deterrence by denial is extremely costly, this constitutes a huge obstacle in its wide and efficient application.

With the volume of damage growing, the need for alternative means of deterrence has remained in the focus of cybersecurity efforts. The military also started to reconsider viable options to deter cyberattacks. The prevailing argument in military circles was that offence is the best defence in cyberspace, as deterrence and defence are both infeasible. The officially published politico-strategic doctrines though—for example the 2011 Department of Defense (DoD) Strategy for Cyberspace or the 2011 DoD Report to Congress—were much more cautious and hardly mentioned offensive capabilities or intent.

Another problem with cyber deterrence is the very wide range of cyberattacks, as opposed to, for example, the range of nuclear attacks. Accordingly, the refinement of the unified Cold War deterrence approach is observable in cybersecurity strategy formulations. This is analogous with the methodology that Freedman determined as narrow deterrence. It is a form of deterrence narrowed down to retaliation against specific actors and certain weapons, and focuses on the protection of certain systems. For example, in 2013 the DoD's Defense Science Board (DSB) issued its study on Resilient Military Systems recommending deterrence as a necessary element of a cybersecurity strategy, but only as one complementary element of three other constituents, defence, resilience and offence. It recommended narrow strategic deterrence reserved only against the most menacing nation state cyber threats. [3]

Later, in April 2015 the DoD Cyber Strategy, still defensive in posture, pivoted on deterrence, mainly by denial, but the strategy also speaks about the use of offensive cyber operations much more explicitly then any time earlier, if the protection of the U.S. homeland and U.S. vital interests require. There is a new element, only mentioned in a half-sentence, which is the potential use of cyberattacks as a deterrent against threats from other domains. One set of strategic issues is whether cyberattacks can be used as a legitimate coercive means

not just in response to cyberattacks that is in-kind retaliation, but applied more broadly as a means of "cybered" deterrence.[3] The major argument for using cyberattacks as coercion is that it is bloodless and thus less damaging than a military attack.

The DSB also launched a specific cyber deterrence task force in October 2014 that concluded its report in March 2017 incorporating the experiences of the election meddling. It contains several ideas long having been circulated in academic circles, but occurring in public official reports for the first time. Hence, these parts represent a shift in official strategic thinking rather than real novelty in strategic studies. It furthers the idea of narrow deterrence. Most significantly, it acknowledges that: "a more proactive and systematic approach to U.S. cyber deterrence is urgently needed." [4] The report advocates offensive cyber and non-cyber responses with an unprecedented openness. Instead of a generalized deterrence strategy, the report recommends that deterrence be *tailored* to different adversary groups or specific adversaries (great powers: China, Russia; regional powers: Iran, North Korea; and non-state actors: terrorist groups). In deterrence literature tailored deterrence means: "designed and applied with a specific target's motivations, risk acceptance, worldview, and capabilities in mind." [2: 267] The report also endorses "a wider range of military cyber options, and a clear policy and legal framework for their employment", especially vis-à-vis Russia and China. [4: 9] The United States must systematically develop a portfolio of scalable, military and non-military response options to a wide range of potential cyberattacks and costly cyber intrusions "to be able to rapidly provide the President with a range of cyber and non-cyber response options in situations where deterrence fails. In order to support timely decision-making, the 'plays' in this playbook must be in the context of a clear policy and legal framework for their employment (including policy and legal vetting and evaluation via interagency war gaming and discussion)". [4: 14]

A separate section is devoted in the report to strategic and crisis stability. Given the relatively low level of risk in using first strike against an adversary's military capabilities increases the risk of escalation. Therefore, new rungs have to be inserted into the escalation ladder identified through war gaming experience and bilateral strategic stability talks. The report asserts that "[a] critical element in strengthening the U.S. cyber deterrence posture is the clarification of norms regarding the implantation and employment of offensive cyber weapons." [4: 23]

The 2017 National Defense Authorization Act approved by Congress at the end of 2016, delegates the role directly to the DoD and then to the new President to examine and elaborate more effective military and non-military ways of deterrence and the "descriptions of relevant authorities, rules of engagement, command and control structures, and response plans relating to such options". Within 180 days of receiving the DoD report, the legislation requires the President to report to Congress on cyberattacks that warrant a military response. That report should include a "discussion of the types of actions carried out in cyberspace that may warrant a military response or operation; A description of the role of the military in responding to acts of aggression in cyberspace against the United States; A description of the circumstances required for a military response to a cyberattack against the United States;

[3] Gaycken and Martinelli differentiate "cybered deterrence", as deterrence by cyber means, and "cyber deterrence", as deterrence of cyberattacks. [25]

[and] A plan for articulating a declaratory policy on the use of cyber weapons by the United States." [5]

In late 2013, as part of the 2014 National Defense Authorization Act, Congress called for a declaratory deterrence policy by the President. The White House's Deterrence Strategy, as discussed in the previous section, focuses on hardening and increasing the resilience of the most vital critical infrastructure systems as deterrence by denial. Meanwhile, prioritizes the law-enforcement (investigative and prosecutorial) paradigm, partly modelled on counterterrorism, and economic sanctions as cost imposition. Offensive cyber operations are reserved for the most severe cases.

Retaliation, Attribution and Self-Restraint in Cyberspace

In the cyber context, retaliatory deterrence still has a low political feasibility. Retaliation can be in-kind, meaning a counter cyberattack or cross-domain. For several reasons, the U.S. is inclined to exert self-restraint in using cyber offensively. The fundamental feature that distinguishes cyberspace as a strategic environment from the other domains is the difficulty of attributing the perpetrators, which undermines any quick response options. No comprehensive discussion of attribution studies is possible here. What is important to note here is that attribution capability has become a strategic asset for every state. Technical attribution works by tracing back the computer or its geolocation, it can never be unquestionably exact, thus a good result is rather a matter of degree. Digital forensic investigation has to be supplemented with intelligence and information analysis to provide information about the person and the full profile of the culprit(s), and ultimately their links with states or other entities. The more intelligent sources are involved, the higher level of certainty can be achieved. Good attribution requires an immense amount of resources, both technical, human and political, therefore cost is a highly restrictive condition.

Consequently, attribution is not just technical but also a (geo-)political process, and thus requires a very high level of evidence that stands up to scrutiny. In order to initiate a legal procedure or to justify retaliation in self-defence necessitate both solid evidence that meets some legal standards, and the political clout to convince the international community. It is called the burden of proof in legal parlance, and in absence of legally fully verifiable evidence, attribution is only political. If the cyberattack amounts to a violation of international law, but stays below the level of an armed attack, the victim state still has the right to react by a *countermeasure*, which would otherwise itself violate international law, to induce the other state to stop the acts causing disruption. Countermeasures cannot be forcible and must be proportionate, an in-kind response as close to the original violation as possible. In strategic terms, this would parallel compellence.

In the security studies, the most thorough paper on cybersecurity attribution was written by Thomas Rid and Ben Buchanan. Alluding to the many uncertainties surrounding attribution, they say that attribution is what states make of it. "On a *strategic level*, attribution is a function of what is at stake politically. The political stakes are determined by a range of factors, most importantly by the incurred damage. That damage can be financial, physical, or reputational"—they write. [6: 3] Appraising the effects and thus the appropriate response to a cyberattack, in cases like the election influence operations, when the attack builds up slowly

and incrementally, is even more challenging. In addition, international law actually does not determine the standard of proof for States to undertake countermeasures or other means of self-help.

In the U.S., just like in the election hacking case, the private IT security firms play a significant role in detection, incident management and attribution. Those major threat intelligence companies are in the vanguard of IT security worldwide that gives them credential. Consequently, private sector threat intelligence might be a potential point of reference for nation states, too. However, one must not conflate U.S. public attribution with threat intelligence. It rarely happens publicly, but rather through the specialized and confidential information sharing channels between the government and the private sector. The decision whether to communicate the results or not, and how to do it is part of the strategic decision. Public attribution might result in the offenders' termination of an operation, changing tactics, or reacting publicly to allegations. There is another part of the strategic equation, publicizing attribution is also a sensitive issue as it might compromise intelligence sources and procedures, as well as vulnerabilities of the victim. Attribution capability and public attribution constitute a very important element that supports strategic deterrence, and it has been emphasized since 2011, in every official cyber deterrence study and doctrine. An additional message of the identification and indictment of specific persons, or as in 2016 also their links to the Russian Government is that the U.S. is in the possession of very sophisticated attribution capabilities, even if the method of retaliation is not yet refined.

U.S. deterrence strategy, meaning the political and military posture adopted by decision-makers is aimed at averting military or cyber confrontations at the level of inception in the adversary's mind. Patrick Morgan distinguishes this kind of deterrence as *influence strategy.* Meanwhile, the Russian or Chinese strategic thought, in contrast, uses *control strategy,* aiming to take away the other side's ability to launch an attack. [2: 37–38]

As one of the most digitized nations and with its cyber defence at a nascent phase, the U.S. is highly susceptible to cyberattacks. As James Clapper Director of National Intelligence (DNI) said during a Congressional hearing, you do not throw stones when you live in a glasshouse. Therefore, the U.S. advocates strategic and crisis stability in cyberspace as well, just like in the kinetic domains, focusing on political and diplomatic crisis prevention measures. Besides its vulnerability to cyberattacks, the U.S. benefits a lot from long-term stability in the interconnected commercial and military environment. In the White House's *International Strategy for Cyberspace,* or the Department of State's *International Cyberspace Policy Strategy* and in the Department of State legal adviser's statement entitled *International Law and Stability in Cyberspace,* international stability is a central concept. The U.S. sees itself as a standard bearer in cyber issues as well, and pursues international strategy accordingly. Consequently, the U.S. strives not to set a bad precedent in using cyber operations widely and recklessly.

Once military or cyber confrontation did start, escalation dominance is a primary goal. Cyberattacks are especially problematic in terms of escalation, as the second and third order effects are not sufficiently mapped out; nevertheless, it is widely acknowledged that cyberattacks are prone to swiftly escalate into physical space. It is extremely difficult to plan and implement targeted cyberattacks in order to achieve specific strategic effects, thus nation states tend to use it sparingly. In spite of the laborious efforts of international law experts, the legal background and the rules engagement of offensive cyber operations is still unclear.

Another hindrance in the usage of offensive operations comes from the nature of cyber weapons. As soon as a malware is detected, the defenders can patch the particular vulnerabilities, thus it cannot be used again. In addition, it is only a matter of time and expertise that its patterns are reverse engineered, and rivals can improve themselves and learn new techniques, thus cyber weapons might as well be turned against the attacker. [7]

Retaliatory threat also has to be credible. Nevertheless, due to the above-mentioned reason, nation states try hard to conceal their actual cyber capabilities. As a result, the reluctance to brandish one's cyber force to prove how powerful it is renders deterrence ineffective. Instead, the U.S. announces loudly how it extends the volume and technical skills of its cyber troops, as well as its commitment to use them when called upon. However, the higher-level strategies coming from the DoD and the White House emphasize that a retaliator cyberattack is the last resort.

Finally, the most important fact is, that in-kind retaliation or more broadly an active-defence military response is not guaranteed to be able to efficiently neutralize the threat of an ongoing cyberattack, especially in peacetime. That is, the compellence value of cyberattacks is controversial. Martin Libicki analysed this aspect in depth in his 2009 study on Cyber deterrence: eliminate hackers. Nevertheless, the U.S. military does allot great deterrence value to cyber power when it is preparing to reach its full offensive and defensive cyber operational potential that is superior to any other nation state. [8] [9] The idea is similar to the strategic strike value of the air force, [10] that even if the sources of the threat cannot be neutralized directly, the will of the attacking party can be broken by disrupting military supply chains or decapitating supporting economic facilities, or by imposing unacceptable costs on the attacker's hinterland.

Although the White House's presidential directives, the *Cyber Deterrence Strategy* issued in December 2015, as well as the DoD's *Cyber Strategy* which come to the closest of policy guidance and declaratory strategy, order only a last resort role for the military. This judgement, however, is in flux both at the strategic and the operational level. Military cyber power is developed in parallel as a means of deterrence, along with an incremental overall strategic shift in the intention to use it.

Using the military in retaliation is regarded as a last resort. Obama was well-known for his non-confrontational, cautious but pragmatic attitude. According to officials near him, this outlook dominated major U.S. decisions on how to employ cyberattacks, for example against Libya in 2011 or in response to Iranian DDoS attacks in 2012–2013. Based on Obama's personal statements, this approach prevailed in the Russian case, too in 2016. Self-restraint is also integrated into strategy. In June 2013, the top-secret *Presidential Policy Directive* issued in 2012 was leaked. It establishes cyber operations policy for a number of offensive and defensive cyber operations. Two kinds of operations are enlisted that correspond to power projection or active defence in cyberspace: "Defensive Cyber Effects Operations (DCEO): Operations and related programs or activities—other than network defence or cyber collection—conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks for the purpose of defending or protecting against imminent threats or ongoing attacks or malicious cyber activity against U.S. national interests from inside or outside cyberspace. […] Offensive Cyber Effects Operations (OCEO): Operations and related programs or activities—other than network defense, cyber collection, or DCEO—conducted

by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks." [11: 3]

Cognizant of the challenges due to legal complexities and targeting precision, most of the cyberattacks can only be authorized by the President of the Defense Secretary. In order to avoid collateral damage, including upsetting the stability and security of the Internet, and unintended foreign policy consequences, decisions to attack have to be weighted carefully and measured against all other options. Prospects of an offensive cyberattack against the U.S. private infrastructure have to be considered, too. All in all, the assiduously compiled document arranges for alternatives that minimize the use of OCEO.

Proportionate Response, Legal Considerations and Declaratory Policy

Returning to the issue of proportionate response, the threshold for a retaliatory response is obscure legally and politically as well. The definition of a *major cyber incident* is an approximation of the impacts of cyberattacks on vital U.S. values and interests, and shows how the U.S. thinks about cyberattacks within its jurisdiction. The U.S. is a vocal advocate of the norm that when the attack is safely attributed to a foreign nation state, international law constitutes the main point of reference on how to respond to it. Unfortunately, when it comes to cyberspace, the interpretation of international law is extremely contentious. The U.S. authorities do not automatically recognize the Tallin Manual, where influence operations are mentioned as an act not deemed equivalent to the use of force: "[a]s an example, non-destructive cyber psychological operations intended solely to undermine confidence in a government or economy do not qualify as uses of force." [12: S1, R11, par. 3]

In fact, the U.S. official statements hardly go into any specific details about how international law is applicable in cyberspace. In addition to a few particular policy statements of U.S. Department of State officials, the Law of War Manual is regarded as the most important expression of the U.S. views on the law of war, and it is also the most detailed, publicly available record of U.S. legal guidance on cyber operations since a legal assessment published by the DoD Office of General Counsel in 1999. [13] What the Obama Administration defines as calculated ambiguity, is most visible in the omissions or the vagueness of the Manual. It is inarticulate on what kind of cyber operations the use of force is needed, and also on the standards of attribution. What constitutes a lawful target in cyberspace is not discussed in detail either. At one place, the Manual notes that cyber operations which merely involve information gathering may not implicate rules applicable to attacks. What amounts to an attack is not discussed in detail, it is only mentioned in the context of cyber operations. In accordance with an apparent majority of international lawyers, the Manual reserves the application of the *ius in bello* rules on targeting to operations that amount to an attack. The Manual refers to a cyber operation "that would destroy enemy computer systems" as prohibited if directed against civilian infrastructure. The Manual notes that rules that apply to attacks do not apply to operations below the attack threshold and such operations may therefore be directed, consistent with the law of war, against civilians or civilian objects subject to the requirement of military necessity. The Manual mentions briefly that cyber operations resulting only in reversible or temporary effects may not amount to an attack. Such operations can be webpage

defacement, disruption of Internet services and dissemination of propaganda. Proportionality in *ius in bello* prohibits attacks expected to produce "loss of life or injury to civilians, and damage to civilian objects incidental to the attack" that would be "excessive in relation to the concrete and direct military advantage expected to be gained". The Manual dismisses from proportionality calculations, "mere inconveniences or temporary losses" including "brief disruption of internet services to civilians" as well as "economic harms in the belligerent state resulting from such disruptions". [13]

Thresholds have to be effective in a strategic sense too, and thus need wider international recognition. According to a RAND study a threshold is: "…a negotiated, declared, or tacitly understood delimiter between measures short of war and high-order conflict such as full-scale conventional or nuclear war." [14]

Clearly articulated policy is indispensable in strategic planning to give unified and unambiguous guidance to lower-level strategies. Explicit or declaratory policy is very often demanded from the President by the domestic military, legislative and expert community. In the international context, clarity is key in governing alliance policies and in signalling to rival nations. If there is no common interpretation of signalling acts, then the whole effort is useless, or might become even escalatory.

The declaratory policy based on the nuclear analogy (Nuclear Posture Review) states, in general terms, why a nation obtains certain kinds of weapons and how those weapons will be used. Offensive cyber operations and intelligence gathering are not new, but in contrast to earlier time periods when they were developed and used in complete secrecy, now their use for national security purposes is gradually gaining some legitimacy and thus require mutually acknowledged international rules. The U.S., however, is highly secretive about its cyber weapons policy. In comparison, Russia and China speak much more openly about how they want to employ their cyber capabilities. Secrecy is inherent in U.S. cyber policy. The White House during the George W. Bush Administration started to partly unveil its strategic intentions in cyberspace. The Obama national security administration realized the need and was much more open, but still refused to set precisely what the U.S. regards an armed attack in cyberspace, and advocated *calculated strategic ambiguity* instead to maintain some freedom to manoeuvre. The 2015 White House report to Congress articulates the need for "a nuanced and graduated declaratory policy and strategic communications" tactic that emphasizes the U.S. Government's commitment to using its capabilities to defend against cyberattacks, but one that is "ambiguous on thresholds for response and consequences to discourage pre-emption or malicious cyber activities just below the threshold for response. […] The administration will consider whether to speak more openly about whether and how the United States might respond to malicious cyber activities, although such public discussion will require carefully balancing such transparency against intelligence and military equities…" the report states. [15: 3]

A DNI officials responsible for cybersecurity commented on the White House official policy: "You don't want to invite people to do anything they want below that red line thinking they'll be able to do it with impunity, and secondly, you don't want to back yourself into a strategic corner where you have to respond if they do something above that red line or else lose credibility in a geopolitical sense. […] There's an interest in ambiguity from a strategic sense that also leads to a strategic uncertainty. So it's two sides of the same coin […] If you

don't have specific red lines, you don't have specific necessarily action plans in certain scenarios." [16]

Moreover, there is a consensus that a response also has a publicly undisclosed element, presumably cyber in nature. In 2014, North Korea's Internet network was also knocked out for almost hours. Russia was subject to several cyberattacks between October and December 2016, but there is no evidence they had any link to the skirmish between Washington and Moscow. [17] This reasoning aligns with what Libicki described as *implicit deterrence,* and as the best possible strategic option for the same reason as the U.S. Government stated.

In cyberspace, uncertainty is ubiquitous, and thus calculated ambiguity is difficult. Traditionally, strategic ambiguity means that nation states intentionally leave certain parts of their strategic choices unveiled, when they want to avoid having to choose between opposing options and thus forgo having to "pay an opportunity cost" of lost choice or bear the negative consequences of their strategic choice. The doubt so created also liberates other states who can pretend not to know and thus not having to react publicly to the undisclosed facts, but still being aware they can take those facts into account when planning their own actions. Given the substantial amount of uncertainty in cyberspace, and the volume and scope of cyberattacks against U.S. infrastructure, this strategy rather encourages others who may think they can get away with attacks, or the costs stay below the gains. As a result, U.S. strategic ambiguity seems to be more of a genuine nature than calculated.

Consequently, it is no surprise that President Obama even in possession of good enough attribution tends to first discuss the issue behind closed doors, only at the highest level with the attacking state, as he did so with China and also with Putin at the G20 summit in October 2016. Simultaneously, signalling might also be conducted through public or non-public channels. However, similarly exploiting plausible deniability, the U.S. is still supposed to carry out the most of its cyber activities in secret.

As a matter of fact, the majority of cyberattacks in a calculated manner stay below the level that could possibly reach the damage caused by an armed attack. So did the 2016 Russian operations. Michael Schmitt, a leading legal expert on cyberattacks said: "That lack of clarity is an invitation for Russia and other aggressors to launch similar operations. If states don't, frankly, move forward with a little more dispatch and a little more focus, our opponents are going to play in this gray area." [18]

At the heart of the legal matter is, whether the Russian interference amounted to a violation of the international law. First, it would qualify as such, if it is regarded as a coercive intervention into the internal affairs of another state that is force the target state to do something it otherwise would not do. In the Russian case this coercive element is the most contentious. The intervention could be considered coercive if there was unambiguous evidence that Russia's intent was to alter the result of the elections in favour of one of the candidates. Whereas, the Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence (ODNI) on Election Security states that Russia's intent was to undermine the integrity of the election. Later, the ODNI declassified report entitled *Assessing Russian Activities and Intentions in Recent US Elections* "explicitly stated it couldn't determine the effect of the suspected Russian influence campaign on the election process." [19]

Second option is the violation of U.S. sovereignty. Sovereignty guarantees that states have the exclusive right to control their territory. Unauthorized intrusion into the computer

system of another country might amount to the breach of sovereignty, but this runs counter to the consensual view of turning a blind eye over espionage which in this case was also accompanied by the leak of information. Still that doubtfully amounts to the violation of sovereignty.

If the atrocity does not violate international law, the target state still has the right to "retorsions" under international law. These are actions that states can adopt as self-help without violating their international law obligations. Actually, U.S. response measures fall into this category, and U.S. charges do not explicitly mention that Russia committed a violation of international law. As legal experts point out, retorsions, unlike self-help measures do not even have to be proportionate and thus they can be applied with much more freedom.

Elections as the Target of Cyber-Enabled Influence Operations

National elections are always politically sensitive time periods and the widely spread digitized platforms open up new access points to manipulation. The technical vulnerabilities of voting systems have been a subject of worries since earlier times. In 2008, large amount of information was stolen from the computers of the Obama and McCain campaign teams. Experts have called attention to the vulnerability of the electronic voting systems; still little precautions had been made to introduce more trustworthy systems. [19] There is no consensus on to what extent direct manipulation of election systems can influence final election results. There is no unified national voting system in the United States. Voting systems vary by state and local entities. The biggest concerns are vulnerabilities in voter registration databases, where voters and tabulation systems can be disenfranchised, which happened in a 2014 Ukrainian election, and attackers infiltrated some voting machines and registries in the U.S., as well. In close contests, experts say, it is enough to manipulate the number of legitimate voters in battleground states.

Releasing sensitive information or the spread of fake news to manipulate public opinion are also tactics seen before. The real tactical novelty was the wide spread systematic social media manipulation, as well as the willingness of the perpetrators to reveal their presence, although not their true identity. [20]

Early in January 2017, the U.S. Congress verified and acknowledged the result of the 2016 elections as valid, and the intelligence community fell short of claiming that the Russian influence operations did manage to alter the final election results. Therefore, from a legal perspective it would be difficult to prove that Russia breached U.S. sovereignty and achieved decisive strategic victory over. Hence, in a strategic sense, the purpose of the meddling has to be sought elsewhere.

Due to the attribution caveat, the dubious legitimacy of counteractions, and the low cost-high gain ratio of elections meddling render elections even more geopolitically worthwhile soft targets. In this case, doubt and suspicions about the integrity of the election was dispensed. IT security and intelligence experts claimed that the perpetrators did want to be noticed, or even advertised their theft. Consequently, the operation can also demonstrate that the attacker has sophisticated cyber capabilities on a par with the U.S., and is not afraid to use it to exert influence. Accordingly, validating its own major power status that merit a strategic partnership role. Holding national elections integrity in danger can also serve

as a deterrent. As diplomatic relations between the U.S. and Russia has been deteriorating since at least 2011, and they reached a low point in 2016. In the Russian view, Russia is in a constant state of war with the West. Even at the time of lower level tensions, Russia has been alleged to use DDoS or defacement attacks in coercion or to express its resentment. In his seminal work entitled *Strategy of Conflict*, Schelling argues that strategy in the nuclear age was less about the application of force and more about the "exploitation of potential force". Competitors sought to coerce each other through threats. The power to make threats was not reducible to capabilities or clear commitments alone. Rather, one could also gain leverage through deception and bluffing. That is, you could manipulate the other party and gain a concession. The art of strategy involved constraining an adversary's attacks by manipulating their expectations of costs and risks.

But like, for example, in the attack against Georgia in 2008, the political turmoil might serve as a prelude to a military attack, preparing the battlefield for a larger campaign. Election meddling or similar cyber enabled influence operations have a high strategic value. The long-term strategic question is, therefore, if such operations are to be tolerated tacitly as a useful form of coercion, less damaging than military confrontation.

International Strategy

In line with the main aim of this study, the U.S. election hacking is contextualized in a comprehensive strategic context. Hence, since the beginning of 2000, U.S. has sought to reach out to its allies and international partners employing diplomatic means in its cyberspace policy. The Obama Administration has been especially active in its efforts to elevate cyberattacks into the realm of strategic-politico thinking and shape the global strategic environment through the promotion of international law and norms of behaviour in cyberspace. The U.S. advocates a set of non-binding voluntary norms articulated in the 2011 White House International Strategy and in several official statements of the DoS. These norms and confidence building measures—initially focusing on common vocabulary, and lately on international stability—are often also interpreted as means of deterrence, or as measures supporting deterrence. In addition, the U.S. is very active in bilateral talks and agreements on contingency cooperation, targeting, information sharing, or international policy coordination, with other countries including China and Russia, or regional organizations like the EU.

The U.S. identifies itself as standard-bearer and global leader whose narrative seeks to reflect universal values and interests. It pictures cyberspace as a wild-wild west, ungoverned territory, where establishing norms of acceptable behaviour is in everybody's interest and those who misbehave can be punished. Accordingly, cyberspace is a globally interconnected and interdependent area—global commons, where the free flow of information and stability is a common good, and disruption is detrimental to all. However, this idea is misplaced or even directly antagonistic with the interests of other states. For example, Russia, China, Iran or North Korea follow a different strategic path that aims to construct self-sustaining IT infrastructures and networks in order to reduce their dependence to a minimum, and to boost their state control over "sovereign" cyberspace to the maximum. Given the Russian great

power identity and adversary relations with the West, any operation that diminishes the moral standing and credibility of the U.S. as a global leader is a strategic gain for Russia.

The prohibition of attacks on critical infrastructure is one of these norms, but before 2016 election systems were not part of it. Furthermore, the U.S. seems somewhat flexible when interpreting these norms. It is indicative, for example, when State Department Deputy Coordinator for Cyber Issues Michele Markoff said that the supposedly Russian attacks on Ukrainian critical infrastructure do not violate these norms because they only apply in peacetime. The U.S. also seeks to ensure its own interests through these norms, but it may well have blowback effects. For example, leniency with cyber espionage or cyber exploitation for national security purposes has actually limited U.S. freedom to sanction and deter substantial but non-disruptive cyber intrusions. In 2015, James Clapper ironically expressed envy over the Office of Personal Management hack's success. Moreover, cyber intrusion techniques used for espionage or exploitation can very easily be turned into disruptive attack mode, thus inhibiting defensive efforts.

Part Conclusion

In light of these strategic, legal and political considerations, the Obama Administration's caution seems to be warranted. In December and January 2016, the Government and the President published several official statements attributing the attacks to the highest levels of the Russian Government and the intelligence services. Technical and non-technical evidence was cited by ODNI, Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), and the Department of Homeland Security (DHS). 35 diplomats were expelled because of a series of unacceptable Russian activities upsetting diplomatic norms of behaviour going back to several years.

The agencies of the widest and highest level, showing unity of effort and consent, provided attribution. The DHS–FBI Joint Analysis Report and the accompanying list of IP addresses manifested for the first time that the U.S. Government acknowledged that the Russian cyber gang names and methods exist (not necessarily all involved in the election hacking) with the aim to raise awareness about Russian malicious cyber activity and thus enable potential targets to better defend themselves. Earlier it was only in the Sony case that a nation state and not just certain individuals were identified as perpetrators in any official statements. The executive order entitled *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities* dates back to 2015. The scope of the original Executive Order is very telling of the U.S. narrowly focused threat perception, concerning activities that:

- harm or significantly compromise the provision of services by entities in a critical infrastructure sector;
- significantly disrupt the availability of a computer or network of computers (for example, through a distributed denial-of-service attack);
- cause a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain (for example, by stealing large quantities of credit card information, trade secrets, or sensitive information).

After the Russian meddling, the order was amended to authorize sanctions on those who:

- tamper with, alter, or cause a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions. [21]

Using this new authority, the President has sanctioned two Russian intelligence services, The Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) and The Federal Security Service of the Russian Federation (FSB), four individual officers of the GRU, and three companies that provided material support to the GRU's cyber operations.

This combined response signified a very important normative message on what is unacceptable behaviour in cyberspace, and what can be expected as proper attribution and proportionate response. In terms of deterrence, the pattern set back in 2015 continued applying a comprehensive cross-domain, whole-of-the nation approach also including some undisclosed most likely cyber response, without escalating the attack.

To sum up, cybersecurity strategy demands a comprehensive strategic approach which involves deterrence only as one of the ways. Currently a non-military posture dominates the U.S. approach, pure cyber defence is combined with deterrence by denial and cost imposition, as well as by wide ranging diplomatic tools. Meanwhile the U.S. cybersecurity efforts, despite several centralizing measures, are still disjoint and reactive, but once an incident is deemed serious enough, response is deliberated carefully and on an overall strategic basis considering effects to wider foreign policy and national interests. Reducing uncertainty deriving from the strategic environment should be a central principle in a security strategy, and in particular in cyberspace. Accordingly, the lack of clear declaratory policy, or the so called calculated strategic ambiguity at the highest level of strategic hierarchy results in disorientation at lower the strategic levels too. Moreover, it impairs overall deterrence. The U.S. socio-political and strategic culture is inherently decentralized, therefore, allocating responsibility for cybersecurity at lower state and local (commercial) levels is a trend to be expected in future policies.

Digitally enabled national elections present a particularly attractive target for politically motivated influence operations, and the integrity of elections is vital for political order. Therefore, elections security or more broadly political security[4] need to be integrated into national security concepts. As cyber-enabled influence operation is likely to remain a strategic threat, besides the technical verification solutions, the United States should outline a clear declaratory policy on electoral interference that entails cost imposition.

Strategic Cultural Context

National security strategic planning pivots on the accurate assessment of the strategic environment, and thus on the catalogue of *real* threats coming from it. Threat perception and the choice of how a nation state aims to address those threats at a strategic level are influenced by the distinctive historical experiences, domestic political environment and

[4] In securitization theory, political security is about the organizational stability of social order. The heart of the political security is made up of non-military threats to sovereignty. [26: 141]

technical determinants. In 2016, although there were plenty of indications that Russia had been making attempts to influence U.S. elections, the actual incidents caught the U.S. national security and political elites off guard, therefore rendering response completely reactive. As a recent precedent, in 2014 Russia had targeted public opinion and rigged elections in Ukraine. Moreover, U.S. intelligence had been tracking specific Russian attempts to access U.S. voting systems, although it is not publicly known how much of that was reported to the parties concerned. [19]

Besides the disjoint domestic cybersecurity governance and the calculated strategic ambiguity, the U.S. was taken by strategic surprise due to a narrow strategic focus on threats coming from cyberspace. This limited focus might be ascribed to long-running Western biases towards the strategic cyberattack concept and cyber power concepts, as well as to the rigid binary view of war or peace state of affairs. A detailed comparison of Western and non-Western strategic approach to cybersecurity is beyond the scope of this study. Instead, we provide a brief outline of some major differences in the American and Russian cybersecurity orientation that might explain heightened U.S. susceptibility to Russian political influence operations.

The Evolution of U.S. Threat Perception in Cyberspace

In the U.S., cyberspace had been securitized gradually over the past decades, and its roots go back to times before the Internet, to at least as early as the 1970s. In the U.S. cybersecurity approach, hard power assets like military and economic security have been traditionally strategized as vital U.S. interests. As a result, by the second part of the 1990s, the idea of strategic information warfare (SIW) became widespread. Computer scientists repeatedly warned of the vulnerabilities of the growing number of networked computer systems, for example, one landmark study was the National Research Council report in 1991 *Computers at Risk: Safe Computing in the Information Age.* By the mid-1990s, simultaneously with the accumulation of sophisticated cyberattacks against high-end U.S. governmental or military computer systems, the technical information security risks were increasingly linked with the societal and political impacts. In the military strategic planning, the concepts of the Revolution in Military Affairs and information operations gained ground. The intelligence community has been sending alarms about extensive foreign power cyber espionage. Both in the academic and military strategic community the notion of information warfare has been widely explored. George Rattray points out, though, that information warfare was (is) a broad construct, and it can be interpreted in many different ways. [10] However, by the mid-1990s the national security community became preoccupied by the idea of a strategic level information warfare. In terms of strategic studies, the idea was that the enemy can bring a whole country to its knees without an all-out war by targeting its centre of gravity, in this case, the homeland critical infrastructure and/or the military C2 supply and logistic chains. The spectre of a "digital Pearl Harbor", the idea of a sudden, unexpected devastation by comprehensive cyberattacks on critical infrastructure, or the idea of cyberattacks used as "weapons of mass disruption" soon proliferated in national security discourse.

The other area where the U.S. is particularly sensitive to cyber intrusions is the economy. Maintaining U.S. predominance in the global economic production is conditioned to a large extent on its edge in technology and innovation, and its protection is a vital national interest. Consequently, in the U.S. economic security is closely related to intellectual property protection and economic competition is prone to be securitized in terms of national security threat. Before long, in the U.S., narrative large-scale state sponsored economic cyber espionage became labelled as geopolitical competition waged through strategic information warfare. It is regarded strategically significant, and often referred to as "death by thousand cuts" because of the potential effect on large number of people and the ability of states to conduct their economic and military activities globally. [10]

This fear of state-sponsored economic espionage and illicit technology transfer has been detectable in the U.S. since the 1970s, and it has become especially prevalent after 2000. [10: 26] For example, the United States–China Economic and Security Review Commission was created by Congress in October 2000 with the mandate to monitor, investigate, and submit to Congress an annual report on the national security implications of the bilateral trade and economic relationship between the U.S. and China. Each year the Commission submits a detailed report on Chinese economic espionage. In 2011, the Office of the National Counterintelligence Executive in a special report to Congress singled-out Chinese and Russian hackers as the world's most rampant perpetrators on cyber espionage. Economic security is designated as a priority in all the national cybersecurity strategic documents. Such approach conflates the traditional economic warfare concept with cyberespionage, cybercrime, cyber-sabotage and even cyberterrorism. [22] As Paul Cornish, British strategic expert points out, the question is "whether the economy might be the way, and cyberspace the means with which to attack the organization and coherence of a modern developed state; not for financial or criminal gain, and not in order to achieve a terrorist 'spectacular', but for maximal political or strategic ends?" As opposed to "a cyber Armageddon", supposes that "it could be in the economic interests of the predator to preserve and exploit, rather than attack and destroy the target economy and its cyber infrastructure"—says Cornish. [23: 9–10]

Strategic cyberwar concept is modelled upon kinetic strategic warfare conducted with nuclear or the air power, and its impact is clearly felt in U.S. cyber threat perception. Focusing on SIW sets a very high bar to a strategic-level defence or response to cyberattacks, whereas the likelihood of such a high-end attack is rather low, and even non-disruptive attacks, like the election meddling can have significant strategic effects. In all of the publicly available strategic documents or expert opinions up till 2017, this narrow strategic approach prevails. The scope of threats is also narrowed down to the military and economic sectors of security, and political security does not feature as a high priority security threat. For instance, the 2015 WH report on deterrence says: "Although cyberattacks can have a range of direct and indirect effects that vary in their severity, U.S. deterrence efforts are particularly focused on those attacks that could result in loss of life, harm to U.S. critical infrastructure, significant damage to property, or significant threats to the national security, foreign policy, or economic health or financial stability of the United States or its interests." [15: 6]

Although U.S. strategists consider Russia a peer competitor in cyberspace, their strategic calculus seems to disregard the essence of Russian strategic thought. National security level cyberattacks are interpreted as destructive or disruptive activities, or as egregious espionage. Treating major malicious activities in cyberspace as the use of force or armed

attack is dubious, and the majority of the attacks fall below this level. Consequently, efforts to address these activities will not fit easily into delineations and authorities—for example Title 10, Title 22, Title 50 of U.S. Code—defined on the basis of whether it is time of peace or war. Furthermore, while unauthorized access to the servers of the Democratic National Convention (DNC), the Democratic Congressional Campaign Committee and some state election systems, or to the NSA could have been interpreted as "standard" national security espionage operations, the leaking of carefully selected sensitive information aims at different strategic gains. These activities amount to covert action and incorporate influence operation or active measures well-established in Russian strategic thinking.

It was only after the elections fiasco that there has been a shift towards a more nuanced U.S. strategic approach. The 2017 report of the DSB Task Force on Cyber Deterrence addresses these challenges. It says that cyber deterrence must be able to cope with a range of cyberattacks, and "…it must do so in contexts ranging from peacetime to 'grey zone' conflicts to crisis to war". [4: 9] Accordingly, the report distinguishes two major categories of cyberattack: "*Cyberattack:* For the purposes of this report, a cyberattack is any deliberate action that affects the desired availability and/or integrity of data or information systems integral to operational outcomes of a given organization. Not all cyber intrusions constitute attacks; indeed, the vast majority do not. […] In addition, while there is considerable attention given to cyberattacks focused on data and software-in-operation, supply chain vulnerabilities are of growing concern." [4: 2–3]

"*Costly Cyber Intrusions:* Under our definitions, China's massive cyber theft of U.S. intellectual property and Russia's hack of U.S. political parties to facilitate information operations undermining confidence in U.S. elections represent costly cyber intrusions. The cyber intrusions in these cases did not affect the availability and/or integrity of U.S. data or information systems, and so do not constitute cyberattacks, but these intrusions did facilitate unacceptable actions by China and Russia that imposed respectively economic and political costs on the United States." [4: 3]

The report recommends that the threshold for a response and the scope of deterrence should be broadened: "The United States must clarify, first internally and then to potential adversaries, that it seeks to deter and will aim to impose countervailing costs in response to some forms of costly cyber intrusions. Theft of IP and hacking in support of undermining U.S. political institutions are now clearly on the list; there are numerous other contenders. One example is egregious behaviour in conducting cyber espionage. […] Some would view the 2015 cyber heist from the Office of Personnel Management of some 18 million records containing personal information as so egregious as to warrant a strong U.S. response. A second example is the pre-positioning of malicious software in critical systems, for example the HAVEX9 and BlackEnergy10 malware discovered in the U.S. electrical grid. In the view of this Task Force, although egregious cyber espionage and the insertion of malware in critical systems of the U.S. electrical grid may not constitute cyberattacks, the United States must consider how such malign acts might be deterred." [4: 7]

Conclusion

To draw a final conclusion, it can be stated that the strategic appraisal of cyberspace along with the preparation of the institutional and regulatory measures have been an ongoing process for several decades. Nevertheless, there is still a long way to go in order to achieve a coherent policy or genuine strategic planning. As the shortfalls of the response to the Russian meddling show, despite its wide-ranging intelligence capabilities, the U.S. threat perception is rather limited most probably due to its strategic cultural impulses. At the same time, Russia has managed to better align its broader strategic goals with their ways-ends-means triad.

What can be perceived as a granular tendency is a shift towards federal centralization and the general recognition that the government must have a larger role in prevention, information sharing and a much more refined crisis communication. Also, there is a growing willingness to make public attribution and to involve vibrant international cooperation.

References

[1] *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* Washington, D.C.: U.S. National Research Council, 2010. https://doi.org/10.17226/12997

[2] PAUL, T. V., MORGAN, P. M., WIRTZ, J. J.: *Complex Deterrence: Strategy in the Global Age*. Chicago: University of Chicago Press, 2009. https://doi.org/10.7208/chicago/9780226650043.001.0001

[3] *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat.* Washington, D.C.: DoD Defense Science Board, 2013.

[4] *Task Force Report: Cyber Deterrence.* Washington, D.C.: DoD Defense Science Board, 2017.

[5] WEBER, R.: Defense bill sets strict deadlines for Trump to asses vulnerabilities, deter cyberattacks. *Inside Cybersecurity*, December 28, 2016. https://insidecybersecurity.com/daily-news/defense-bill-sets-strict-deadlines-trump-assess-vulnerabilities-deter-cyber-attacks (Downloaded: 24.02.2017)

[6] RID, T., BUCHANAN, B.: Attributing Cyber Attacks. *The Journal of Strategic Studies*, 38 1–2 (2015), 4–37. dx.doi.org/10.1080/01402390.2014.977382 (Downloaded: 20.12.2016) https://doi.org/10.1080/01402390.2014.977382

[7] DÉVAI, D.: Proliferation of Offensive Cyber Weapons. Strategic Implications and Non-Proliferation Assumptions. *Academic and Applied Research in Military and Public Management Science*, 15 1 (2016), 61–75.

[8] KRAMER, F., STUART, H., WENTZ, L.: *Cyberpower and National Security.* Washington, D.C.: NDU Press, 2009. https://doi.org/10.2307/j.ctt1djmhj1

[9] DAVIS, P.: *Cyber Deterrence: An Old Concept in a New Domain.* (Strategy Research Project) Carlsisle, Pennsylvania: U.S. Army War College, 2013.

[10] RATTRAY, G.: *Strategic Warfare in Cyberspace*. Cambridge, Massachusetts: MIT Press, 2001.

[11] *Presidential Policy Directive 20. US Cyber Operations Policy.* 2013. https://fas.org/irp/offdocs/ppd/ppd-20.pdf p.3 (Downloaded: 25.02.2015)
[12] *Tallinn Manual on the International Law Applicable to Cyber Warfare.* (NATO Cooperative Cyber Defence Centre of Excellence) Cambridge: Cambridge University Press, 2013. https://doi.org/10.1017/CBO9781139169288
[13] WATTS, W.: Cyber Law Development and the United States Law of War Manual, International Cyber Norms: Legal, Policy & Industry Perspectives. In. OSULA, A-M., RÕIGAS, H. (Eds.): *NATO CCD COE Publications.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2016. 49–63.
[14] *RAND Stretching and Exploiting Thresholds for High-Order War.* 2016.
[15] *White House report to Congress on cyber deterrence.* 2015. https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/dec2015/cs2015_0133.pdf (Downloaded: 25.02.2015)
[16] MOORE, J. (2015): Here's the Government's New Definition of a Major Cyber-incident. *Nextgov,* November 4, 2015. www.nextgov.com/cybersecurity/2015/11/heres-governments-new-definition-major-cyber-incident/123393/ (Downloaded: 25.02.2016)
[17] LOWE, C., ZINETS, N.: Russia says foreign spies plan cyberattack on banking system. *Reuters*, Dec 2, 2016. https://www.reuters.com/article/us-russia-cyberattack-banks-idUSKBN13R0NG (Downloaded: 25.02.2015)
[18] MARKS, J.: There's Cyberwar and Then There's the Big Legal Gray Area. February 9, 2017. Nextgov. www.nextgov.com/cybersecurity/2017/02/theres-cyberwar-and-then-theres-big-legal-gray-area/135298/. (Downloaded: 25.02.2017)
[19] *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution.* Intelligence Community Assessment, 2017. www.dni.gov/files/documents/ICA_2017_01.pdf (Downloaded: 12.12.2017)
[20] *JAR–16–20296. GRIZZLY STEPPE – Russian Malicious Cyber Activity.* Washington, D.C.: U.S. Department of Homeland Security and Federal Bureau of Investigation, 2016.
[21] *Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment.* Washington, D.C.: The White House, Office of the Press Secretary, December 29, 2016 https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and (Downloaded: 14.01.2015)
[22] RAVICH, S. F. (Ed.): *Cyber-Enabled Economic Warfare: An Evolving Challenge.* Washington, D.C.: Hudson Institute, 2015 www.hudson.org/research/11408-cyber-enabled-economic-warfare-an-evolving-challenge (Downloaded: 14.05.2016)
[23] CORNISH, P.: *The Vulnerabilities of Developed States to Economic Cyber Warfare.* London: Chatham House, 2011. www.chathamhouse.org/sites/files/chathamhouse/0611wp_cornish.pdf (Downloaded: 14.01.2015)
[24] GAYCKEN, S., MARTELLINI, M.: Cyber as Deterrent. In. MARTELLINI, M. (Ed.): *Deterrence and IT Protection for Critical Infrastructures.* Heidelberg: Springer, 2013. 1–10. https://doi.org/10.1007/978-3-319-02279-6_1
[25] BUZAN, B., WÆVER, O., WILDE, J. de: *Security. A new framework for analysis.* London: Lynne Rienner Publishers, 1998.