DOI: 10.32565/aarms.2019.1.3

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

(Part 1)[1]

Dóra DÉVAI[2]

Due to the heightened political sensitivity caused by the recently held U.S. midterm elections and the frenzied media concentration on the 2016 election meddling, hacking and leaks have been in the focus of public discussions ever since. In order to better comprehend the appraisal of the U.S. political leadership back in 2016 and early in 2017, this article contextualizes the events and the response measures in the wider cybersecurity position of the U.S. Tracking down the development of the U.S. political and military approach to cyber threats,[3] we came to the conclusion that the U.S. is lacking a working cybersecurity policy largely because its perception of cyber threats is self-centred and still deeply rooted in the strategic thinking of nuclear or traditional military attacks. Even if the same strategic principles are valid in cyberspace, cyberattacks, single, systemic or part of a broader influence operation, they play out according to a set of completely different dynamics than kinetic attacks. The true strategic lesson of the recent election meddling is that Russia has been, and most probably will be, able to seize the momentum and masterfully exploit those inherent deficiencies. Consequently, cyberspace as a strategic environment necessitates the careful analysis of the strategic thinking of the potential adverse nation.

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

[1] This is the first part of a series of three articles. The second part gives a strategic insight into the national response policy options to substantial cyberattacks in the U.S. The third part of the series 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

[3] The article refers back to the regulatory background at its given state back at the time during the 2016 mid-term elections.

Introduction

“Barack Obama and Joe Biden will ensure that his administration develops a Cyber Security Strategy that ensures that we have the ability to identify our attackers and a plan for how to respond that will be measured but effective” read the 2008 election site of then candidate Barack Obama. [1] The securitization and strategizing of cyberattacks go back to at least as early as the beginning of the 1990s. Nevertheless, there is a growing evidence that nation states have used cyberspace for intelligence and military purposes since the first versions of computers appeared.[4] In the meantime, the dependence of the nation states on the flawless operation of the internet and information technology in general has skyrocketed. In realization of this fact, cyberspace has been publicly recognized as an *operational domain,* and its strategic utility meaning, *the systematic employment of cyberattacks to pursue national political purposes,* has been gaining ground since at least the attack against Estonia in 2007. Moreover, there is also a competition between states seeking to find ways to gain *strategic advantage* through cyberspace that is to use cyber intrusions and cyberattacks in order to influence the “overall relative power relationship of opponents that enables one nation or group of nations effectively to control the course of a military or political situation”. [2: 522] This broadening of the activities of nation states in cyberspace necessitates a novel, more systematic approach beyond military planning, more akin to traditional statecraft and strategic art. Consequently, both in the emerging academic strategic literature and in the evolving politico-strategic thinking of the nation states, the nature of cyberspace and its strategic implications are being widely appraised.

The Evolving Concept of Cyberspace as a Strategic Environment

Cyberspace as a *strategic environment* has distinctive features with still plenty of *known and unknown unknowns.* [3] It is to a large extent a hidden landscape both literally, due to the attribution challenge and the technical complexities, and in terms of strategic thinking, as a result of the fast-paced development of the technology and the nascent strategic thought trailing behind it, but also to the particularly strong secrecy surrounding the cyber activities of the nation states. As national cyber strategies are gradually formulated and simultaneously tested also in real life, these tests and incidents yield pragmatic lessons on the nature and the limitations of distinctive national approaches. The recent events of Russian influence operations during the U.S. presidential elections served as the latest reminder of how distinctive this comprehension can be.[5] One aim of this study series is to examine if the traditions of national strategic thinking.

[4] See, for example: KHALILZAD, Z., WHITE, J. P., MARSHALL, A. W.: *Strategic Appraisal. The Changing Role of Information in Warfare.* Santa Monica: Rand Corporation, 1999. Also: HUNT, E.: U.S. Government Computer Penetration Programs and the Implications for Cyberwar. *IEEE Annals of the History of Computing,* 34 3 (2012), 4–21. NYE, J. S. Jr.: Nuclear Lessons for Cyber Security? In. *Strategic Studies Quarterly.* Washington, D.C.: Air University Press, 2011.

[5] As for the identity and purpose of the Democratic National Committee (DNC), hackers and leakers, there still are some dissenting voices. Based on the joint U.S. intelligence community reports published in December 2016 and January 2017, the author of this article adopts these as proven facts.

In addition, scholars can also have more insight into how cyberspace or the information environment is gaining *strategic sense,* and how it affects the way international conflicts and rivalry take place. At the heart of these strategic discussions, one of the questions splitting Western academic strategists is: to what extent generic strategic theory—and its major concepts like deterrence—is applicable in cyberspace. According to, for example, Colin S. Gray a most renowned British classic strategic theorist, the nature of political power and rivalry remains the same, thus the traditional premises of strategic theory are also applicable in cyberspace. [3]

In light of these tendencies, despite its technological superiority, the U.S. susceptibility and inept response to the 2016 Russian influence operations constitutes an excellent case study of how nation states seek to integrate cyberspace into their strategic thought. In other words, how they intend to maximize their chances to exploit the opportunities in cyberspace in order to realize their national interests; how they perceive threats coming through cyberspace and how they try to neutralize or eliminate them; and also how these distinctive approaches play out against each other. This time, Russia did manage to take the most advanced cyber nation off guard and exert some influence over the integrity of its core democratic political institution. The assumption of this article is that the Russian strategists recognized and exploited the opportunity offered by the inherent technical determinants of cyberspace, as well as the strategic, legal and institutional and doctrinal incoherence and imbalances of the U.S. thinking.

Moreover, although the operationalization of (cyber) informational power in Russian strategic thinking is indeed fundamentally different from the Western approach, the recent developments also prove the long-running knowledge in strategic communities that Russian strategists are "good Clausewitzians" to be true also in cyberspace. As James J. Wirtz from the Naval Postgraduate School puts it, they understand that war is a political act, hence "quick to think through the links between technology, military operations, strategy, and ultimately political outcomes, despite their lack of technological dexterity". [4: 32] Meanwhile, the U.S. seems to carry on the same deficiency as in its kinetic strategic thought. According to a U.S. expert's recent comment, "America's primary weakness is not in its lack of economic or military power, but in a failure to formulate strategy and, frankly, poorly informed decision-making, even when faced with a peer nuclear power. Military capability in and of itself will not fix these cardinal weaknesses in judgment, nor make up for a lack of vision and political will to see hard choices through". [5]

Several guidebooks and manuals have been published recently on national cybersecurity strategy models. In these, crisis management and contingency planning, information assurance, and resiliency are central organizing elements. In this article the focus is different. We argue that the election-time influence operation revealed that there should be an urgent shift in national cyber security thinking informed by the logic of general strategic thinking. Through the example of the American response measures, our aim is to ascertain some of the new strategic challenges in cyberspace including a powerful and assertive adverse nation state. To this end, we contextualize the events in terms of the relevant American and Russian strategic documents and policy statements. According to the logic of strategic theory, national capabilities, cyber or other, have a relative value and must be appraised in relational terms. Examining the events through a strategic lens will yield some insight into first, how historically distinctive strategic cultures determine cybersecurity strategy formation, second, how surfacing strategies materialize in practice, and finally, how the resulting action–reaction cycle plays out in cyberspace.

Accordingly, first we apply the basic concepts of strategic theory to cyberspace and cybersecurity. The objective here is to identify the strategic dilemmas of the U.S. response and more broadly, the strategic planning approach in its national cybersecurity efforts. Then, the study will trace back the roots and the strategic repercussions of the idea of strategic cyberattacks in the U.S. In Part 2, the U.S. cybersecurity thinking is examined in terms of deterrence theory and practice. In the kinetic realm, conventional military and strategic nuclear power are pivotal means of deterrence. As the case study in this article reveals, in cyberspace, though it proves to be a much more daunting task, some experts and practitioners even doubt if this is possible at all. Closely related to deterrence, the Russian hacking case adds some lessons on the strategic importance of attribution, as well. To conclude, we sum up the strategic lessons of this case study and make some recommendations accordingly. An upcoming third part of this article intends to highlight in the same vein the major differences concerning U.S. and Russian threat perception in their respective approaches to the strategic use of cyberspace.

Baseline Definitions

Cyber related concepts are still fluid in national security thinking. Even within one policy area, like the military or homeland security, there is a multitude of strategic documents often with inconsistent terminology, which well reflects the fundamental stumbling block of U.S. strategy development in cyber issues. There is a general effort to centralization and unification within each policy area, as well as at the highest overall national security level. Cyber threats pose security threats of a new character that demand strategic level adaptation, but the nature of national security dynamics, however, have not changed because nation states are pursuing strategic goals in cyberspace, just like in other domains. In this study, we will use working definitions that are closest to strategic theory.

Cyberspace

Cyberspace as a working concept here is understood *as part of the overall strategic environment* in which nation states define their ways, ends, and means. In order to better understand the strategic value of cyberspace, the physical, logical and socio-political components have to be considered as an integrated whole. In the evolving strategic studies of cyberspace, the most common model derives from the fusion of a simplified Open Systems Interconnection (OSI) model that characterizes and standardizes the communication functions of a telecommunication or computing system, and a cognitive layer. In 2007, Martin Libicki divided cyberspace into three layers: physical, syntactic and semantic layer. [7] The fourth cognitive or politico-strategic layer encompasses all the actors and their different motivations interests and strategies—military, civilian, commercial individuals, organizations and nation states—who use cyberspace to achieve their goals.

The notion of cyberspace in the U.S. strategic and national security documents has underwent an unsynchronized evolution. Militarily, initially it only appeared publicly in Information Operations documents and it was limited to the technical that is the physical and the syntactic layers. In addition, cyberspace originally constituted only a subfield of the *information environment* and cyber offensive operations constituted one element of military information support operations. However, it has gradually acquired an independent status as a separate domain of operations alongside land, sea, air and space. The first independent doctrine on cyberspace appeared in 2006 entitled *The National Military Strategy for Cyberspace* that treated cyberspace only in terms of its physical components used by the military to implement military operations

In the wider national security context, cyberspace has also evolved gradually but starting out of a purely infrastructural approach. The first seminal occurrences of the vulnerabilities and threats was the Commission on Critical Infrastructure Protection (PCCIP) in 1997. Ever since then, the national security thinking is centred on the cyber security or the physical safety of the infrastructures.[6]

Cyberattack

As of today, in the U.S. there is no official legal definition of a cyberattack. The evolution of the concept of cyberattack in different U.S. strategic documents will be discussed in detail later on. For the purpose of this study, a generic definition of a cyberattack is used taken from one of the most often cited academic sources, the National Research Council's report entitled *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. According to the report, a cyberattack "refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks". [6: 1] This approach is in line with the official U.S. position that does not recognize unauthorized access to computers, or in other words espionage in itself as an attack.[7]

Cybersecurity Strategy

The strategic implications of cyber conflict reach beyond and across the military, intelligence and economic sectors—extending into the high-policy realm of diplomacy and statecraft. Cyberspace at nation-state level is governed by "economic laws of rival resources" and "laws of sovereign jurisdiction and control". [8: 3] Attacks from the physical and semantic layers impact power at the politico-strategic level, while control at the political layer have effects at the other two. Therefore, cybersecurity strategy must follow the logic of national security strategy: "The art and science of developing and using the political, economic,

[6] For example, in 2009 the *National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23)* defines cyberspace: "as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." [21]

[7] The report designates such penetrations as *exploitation.*

social-psychological, and military powers of the state in accordance with policy guidance to create effects that protect or advance national interests relative to other states, actors, or circumstances." [9: 1]

Strategic Planning in Cyberspace

Generic strategic theory is the academic literature on how to *think about* national (security) strategies. Consequently, in this study the strategy formulation model of the U.S. Army War College will be used as an analytical framework to evaluate the evolving U.S. strategic thought and security policy in cyberspace. [9]

In the following section, the most important premises of strategic theory are outlined. Strategic theory applies a holistic and integrative approach. Formulating strategy at the highest levels of the state, that is at grand strategic or the national security level is: "a process that seeks to apply a degree of rationality and linearity to circumstances that may or may not be either. Strategy accomplishes this by expressing its logic in rational, linear terms—*ends, ways, and means.*" [9: 1]

Strategic planning has essential building blocks and an established, coherent procedure. If any of these is missing or not appropriately presented, the national cybersecurity process will stumble:

"From an accurate analysis of the strategic environment, the strategist *determines the threats to and opportunities* for the advancement or protection of these interests. From *policy*, the strategist receives the political leadership's vision, guidance, and priorities of effort in regard to interests. Thus, in constructing a valid strategy, the strategist is bounded by the nature of the strategic environment, the dictates of policy, and the logic of strategy." [9: 73]

Policy dominates strategy by the articulation of the end state and its guidance regarding resources, limitations on actions, or similar considerations. "Strategy cannot be formulated in a policy or intellectual vacuum." [9: 9] Strategy is hierarchical. The political leadership ensures and maintains its control and influence over the instruments of power through the hierarchical nature of state strategy. Clarity and precision are the essentials of a strategy to provide strategic purpose and unity of direction.

"The role of the strategist is to exercise influence over the volatility, manage the uncertainty, simplify the complexity, and resolve the ambiguity, all in terms favourable to the interests of the state and in compliance with policy guidance." [9: 18]

The strategic environment has a predominant role in strategy. In order to best serve purposes of a national strategy at the highest-level *cyberspace* must be considered in its broadest sense. In strategic theory the strategic environment incorporates: "[t]he internal and external context, conditions, relationships, trends, issues, threats, opportunities, interactions, and effects that influence the success of the state in relation to the physical world, *other states and actors, chance,* and the possible futures. […] the role of the strategist is ultimately to advocate actions that will lead to desirable outcomes while avoiding undesirable ones, *the strategist must understand the nature of the environment in order to exert influence within it*". Strategy is subordinate to the nature of the environment. Strategy must identify an appropriate balance among the objectives sought, the methods to pursue the objectives, and the resources available within the particular strategic environment. Strategy must be consistent with the nature of the strategic environment. [9: 17–18; 66]

"The true purpose of strategy is to create favourable effects in support of policy goals for the advancement or protection of national interests. *Strategic effects* are the impact that the accomplishment of strategic objectives has on the environment. Effect flows from strategic performance—the synergy of the objective(s) achieved, the concept(s) employed, and the resources used." [9: 45]

"In strategy formulation, getting the objectives (ends) right matters most! Objectives are the true focus of strategy formulation and, if not properly selected and articulated, a proposed strategy is fundamentally flawed and cannot be effective." [9: 49]

Strategy rests upon the ends, ways and means structure. "Objectives (ends) explain 'what' is to be accomplished. Strategic concepts (ways) answer the big question of 'how' the objectives are to be accomplished by the employment of the instruments of power. They link resources to the objectives by addressing who does what, where, when, how, and why, with the answers to which explaining 'how' an objective will be achieved. […] Resources (means) in strategy formulation set the boundaries for the types and levels of support modalities that will be made available for pursuing concepts of the strategy. In strategy, resources can be tangible or intangible." [9: 69]

The notion of power is a central idea in political science and international relations, military studies and strategic theory, but it has a distinctive meaning in all three. In political science the concept of power has gone through many transformations since pre-WWII times. In essence, it is about influence and control over resources, or directly or indirectly over another party or more broadly over the circumstances of the given situation. As Lawrence Freedman eloquently determines strategy focuses on interplay and balance between the strategic environment, the desired end state and the choice of the right instruments and elements of power:

"The realm of strategy is one of bargaining and persuasion as well as threats and pressure, psychological as well as physical effects, and words as well as deeds. This is why strategy is the central political art. It is about getting more out of a situation than the starting balance of power would suggest. It is the art of creating power." [10: 12]

In U.S. military theory, by contrast, *cyber power* is equivalent to military capabilities and power projection in a given natural domain like air, sea or land, or in case of cyber, the cyber domain. Strategic theory combines the political and military understanding of power: elements (capabilities) and instruments of national power that are employed in order to exercise control over the strategic environment to achieve the desired end state.

"Capabilities refer to the set of resources and assets the state possesses that increase its potential (capacity) to carry out its aims. In conventional warfare terms, capabilities are measured by factors like the country's population, industrial capacity, technological advancement, or the size of its military forces. In cyberspace, capabilities refer to the state's resources and assets that help it achieve its goals in cyberspace such as numbers of hackers, the level of expertise in computer science, and malware sophistication." [11] Power is measured by the actual influence exerted or the outcomes brought about. The strategic purpose of cyber power is to achieve policy objectives.

Strategic theory is related to but different from strategic culture as a discipline. Nevertheless, the theory acknowledges that distinctive national history, culture and worldview all play an important role in strategy formulation. For example, “Western thinking is permeated with the binary logic inherent to Western scientific thought. Binary logic is rooted in Aristotle’s philosophical law that something is either A or ‘not A.’ It cannot be A and ‘not A.’ It is either true or false. Thus in Western science, math, logic, and much of culture, we assume a world of blacks and whites that does not change—this is bivalent logic—two-valuedness”. [9: 43]

The 2016 U.S. Elections and the Russian Influence Operations

The events during the latest U.S. presidential elections is illustrative of the technical, institutional and strategic cultural aspects that might hinder the development of an effective cybersecurity strategy. Detailed analysis of all the U.S. cybersecurity documents is beyond the scope of this study. Instead, in Table 1 the relevant U.S. public statements, marked in bold italics against shaded background, are enlisted in chronological order along with the timeline of the election meddling events. This format enables a quick overview of both the flow events and how they impact the publication of policy statements that try to strategize response mechanisms to a cyberattack. It also helps to elucidate the fact that cyber security strategic planning is at an early phase of progress, still leaving several major strategic gaps unresolved.

Table 1. *A chronology of key events and U.S. strategic documents and policy statements.* [Edited by the author.]

May 2011	White House: International Strategy for Cyberspace
July 2011	DoD Strategy for Operating in Cyberspace
September 2012	DoD: International Law in Cyberspace. Harold Hongju Koh, DOS legal adviser’s statement
2013	DoD Defense Science Board Study: Resilient Military Systems
2013	White House, Presidential Policy Directive (PPD) 21 entitled Critical Infrastructure Security and Resilience
2013	Cyberspace Operations, Joint Publication 3–12(R)
1 April 2015	White House: Executive Order 1396 “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities”
April 2015	DoD: The National Military Strategy of the United States of America
15 April 2015	DoD Cyber Strategy
5 June 2015	DoD Cyber Command: The Commander’s Vision and Guidance for U.S. Cyber Command: Beyond the Build. Delivering Outcomes through Cyberspace
12 June 2015	Law of War Manual—United States Department of Defense
18 December 2015	White House Report to Congress on Cybersecurity Deterrence
March 2016	Department of State International Cyberspace Policy Strategy
Hacking Incidents Start to Appear in Public	
14 June 2016	The Washington Post revealed that “Russian government hackers” had penetrated the computer network of the Democratic National Committee. Crowdstrike technical report published on DNC hacks.
15 June 2016	Guccifer 2.0 crops up in a BlogSpot.

20 June 2016	Mandiant and Fidelis confirmed Crowdstrike's initial findings that Russian intelligence indeed hacked the DNC.
July 2016	Officials announce that the Illinois state online voter registration system is to be shut down following a hack.
13 July 2016	Testimony of Christopher M. E. Painter, Coordinator for Cyber Issues U.S. Department of State Before the House of Representatives Committee on Oversight and Government Reform Subcommittees on Information Security and National Security Hearing on *Digital Acts of War: Evolving the Cybersecurity Conversation.*
13 July 2016	DNC intruders leaked selected files exclusively to The Hill, a Washington outlet for Congress.
22 July 2016	After Trump was officially nominated and before the Democratic National Convention got under way, WikiLeaks published more than 19,000 DNC emails with more than 8,000 attachments.
26 July 2016	PPD–41 Presidential Policy Directive *United States Cyber Incident Coordination.* The directive called for a renewed National Cyber Incident Response Plan that defines a nationwide approach to significant cyber incidents, including threat level assessment and outlines the roles of both federal and non-federal entities.
29 July 2016	Democratic Congressional Campaign Committee (DCCC) server compromise revealed in press. DCCC organizes campaign finances.
1 August 2016	Shadow Brokers announces they hacked National Security Agency (NSA) and stole cyber weapons which they want to sell at auction.
18 August 2016	FBI issues warning of foreign hackers penetrating voter registration database and state election computer systems in Illinois and Arizona.
4–5 September 2016	At the G20 Summit Obama urged Vladimir Putin not to let cyberspace become the "wild, wild west" and "to cut out" cyber intrusion. Obama called on Russia to "act responsibly and start instituting norms" to avoid a Cold War-style escalation, and issued warning that America had "more capacity than anybody, both offensively and defensively".
30 September 2016	*Draft National Cyber Incident Response Plan* is out for public discussion, still in need of codification.
7 October 2016	*Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security* designates Russia, saying hacks of U.S. political groups and individual politicians could only have been done with the authorization of "Russia's most senior" officials and that its intent was to undermine the integrity of the election.
15 October 2016	Joe Biden said in an interview that the U.S. is ready to hit back to Putin. "He'll know it", Mr. Biden added. "And it will be at the time of our choosing. And under the circumstances that have the greatest impact."
30 October 2016	The Shadow Brokers claims that the 306 domains and 352 IP addresses revealed in the dump belong to the Equation Group.
8 November 2016	Presidential elections.
10 November 2016	*International Law and Stability in Cyberspace.* Brian J. Egan, DOS legal adviser statement
9 December 2016	The Washington Post leaked that the Central Intelligence Agency (CIA) had assessed that Russia interfered in the election to tilt the election to Trump. Investigation announced by Obama, POTUS vowed on Friday to "send a clear message to Russia" as both a punishment and a deterrent imposing cost.

16 December 2016	Obama explains at the end-of-year news conference the White House perspective on how to handle the hacks. He says: "And so in early September, when I saw President Putin in China, I felt that the most effective way to ensure that that didn't happen was to talk to him directly and tell him to cut it out, and there were going to be some serious consequences if he didn't. […] But the leaks through WikiLeaks had already occurred. […] We allowed law enforcement and the intelligence community to do its job without political influence. […] With respect to response, my principal goal leading up to the election was making sure that the election itself went off without a hitch, that it was not tarnished, and that it did not feed any sense in the public that somehow tampering had taken place with the actual process of voting."
22 December 2016	Intelligence Committee releases declassified Snowden Report.
29 December 2016	The State Department declared 35 Russian government officials from the Russian Embassy in Washington and the Russian Consulate in San Francisco "persona non grata". Treasury sanctions on individuals for malicious cyber-enabled activities. Joint Department of Homeland Security (DHS), Office of the Director of National Intelligence (ODNI), Federal Bureau of Investigation (FBI) Statement on Russian Malicious Cyber Activity. The Department of Homeland Security and the Federal Bureau of Investigation are releasing a *Joint Analysis Repor*t (JAR) that contains declassified technical information on Russian civilian and military intelligence services' malicious cyber activity. The President has approved an amendment to Executive Order 13964. National Defense Authorization Act for Fiscal Year 2017 approved.
5 January 2017	Directors Clapper and Rogers testified before Congress about the Russian campaign.
6 January 2017	ODNI Declassified report *Assessing Russian Activities and Intentions in Recent U.S. Elections.* The Analytic Process and Cyber Incident Attribution. The review prepared by CIA, FBI, and National Security Agency officials explicitly stated it couldn't determine the effect of the suspected Russian influence campaign on the election process.
12 January 2017	Shadow Brokers tries to sell the hacked cyber weapons again.

Domestic Strategic Environment: Organizational Hindrances of Strategic Planning in Cyberspace

Due to the large number of diverse stakeholders involved, cybersecurity policy is like a multi-dimensional chess play. The ubiquity and the proprietary nature of the potential targets of a cyberattack causes fuzzy scope of jurisdictional responsibilities and policy priorities for strategic level cyber defence. The White House is responsible for the security and the advancement of vital U.S. interests, thus they should provide political coordination and clearly articulated policy guidance at the top of the strategic hierarchy. However, as of today, the U.S. does not have a single cybersecurity strategy. Cybersecurity strategy formulation is a process overarching several policy areas: national security, homeland security and public order. Strategic planning—currently in the phase of risk assessment, vulnerability and threat assessment, and strategic concept development—evolves in parallel in these different policy areas, as well as at state and local levels in accordance with the inherent legal frameworks and institutional culture of each field. Nevertheless, the Obama Administration has taken several substantial steps to further develop an overarching, coherent and more transparent policy approach built on the preliminary cybersecurity measures going back to the 1980s.

Ends, Ways and Means

In cybersecurity governance the homeland security, law enforcement and national security fields are inseparably intertwined. The domestic security authorities are regulated by a patchwork of *domestic laws* which include the Constitution of the United States, federal statutes, and self-executing treaties. This legal framework obliges both government institutions and private individuals, and regulates the division of labour between departments and agencies. According to the Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government: "responsibility for Federal Government cybersecurity is distributed and shared by all agencies; however, specific agencies have additional roles in supporting this mission and ensuring that the Federal Government has the tools, resources, and guidance necessary to make the risk-based decisions necessary to secure their systems. FISMA[8] states that OMB[9] oversees Federal agency information security policies and practices. The OMB Cyber and National Security Unit (OMB Cyber) was created at the beginning of FY[10] 2015 to strengthen Federal cybersecurity." [12: 6]

These are vying for funding with their own distinctive institutional culture. Moreover, a unified strategy has to be accepted and approved by governmental entities at lower levels too, and also by the private sector. Cybersecurity management to a large extent happens at the state level, and any centralization would mean giving up on some of those local prerogatives. For example, in February 2017, New York was the first and so far the only U.S. state to introduce its own cybersecurity policy with some mandatory regulations. Beyond the inherent vulnerability of information technology devices, these proprietary and legislative features make cyber security strategy a daunting task, and constitute a constant vulnerability. As the Russian influence operation demonstrated, even without any destruction or major disruption, significant confusion can be triggered.

Viewed from a strategic lens, the identification of ends, ways and means are far from being sorted out. *Ends* (what to defend) is one of them. The critical infrastructure protection scheme emerged in the mid-1990s due to the realization of the growing dependency on information infrastructures and the risks thereof. It provides the federal government with overarching regulatory authorities in certain vital industries. Twenty years later, basic concepts of the scheme are still contentious. In 2015, the Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government orders the prioritized identification and protection of high value information and assets. In the second part of 2016, the Presidential Commission on Enhancing National Cybersecurity was convened to develop policy recommendations for the next administration. Accordingly, the commission interrogated critical infrastructure owners on what is vital to keep the national economy functioning during a large-scale cyberattack. During the Obama era, the linchpin of the process was established in 2013 via the Executive Order 13636 entitled *Improving Critical Infrastructure Cybersecurity* and Presidential Policy Directive 21 *Critical Infrastructure Security and Resilience* which set out steps to strengthen the security and resilience of the Nation's critical infrastructure.

[8] Federal Information Security Management Act.

[9] Office of Management and Budget.

[10] Financial year.

PPD–21 re-aligned and updated the HSPD–7[11] critical infrastructure sectors established in 2003, and reduced the number from 18 to 16.[12] Election and voting systems, though were designated as critical infrastructure only after the election hacks in 2016. In addition, it is for the first time that critical infrastructure dependency risks are examined in practice. A large-scale three-year long research is carried out at the Idaho National Laboratory of the Energy Department to map the likely ripple effects and the physical impacts of hacks. Similar tests have been initiated to examine how energy sector grid hacks might affect military readiness. [13]

Ways (who does what, where, when, how, and why) is especially problematic in the domestic cybersecurity environment. As we will see in the next chapter, legislation and the White House tend to apply deterrence as an umbrella strategy in an attempt to achieve strategic unity. Homeland security—risk management and incident response—and law enforcement tools serves as deterrence by denial, and cost imposition. Once these remits are decided all the way through, the question of *means* (resources) also becomes clearer. During the 2016 elections, the Democratic National Convention's servers are owned by the party, and the ownership and operation of election machines fall under state autonomy. Even when the cyber intrusion was revealed, there was no regulation in place concerning inter-agency cooperation and information sharing. Figure 1 serves as an illustration of the fragmented cybersecurity decision making authorities at the top-end of the executive branch.

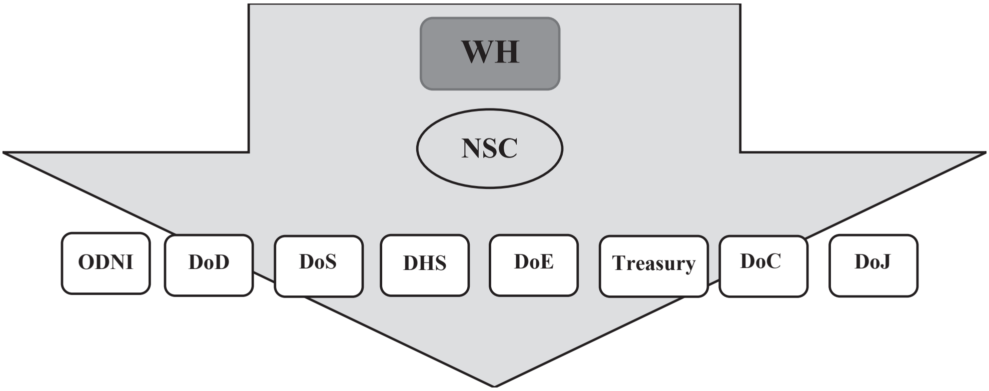


Figure 1. *Politico-strategic cyber security planning at the executive level.*[13]
[Created by the author.]

[11] Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. See: www.dhs.gov/homeland-security-presidential-directive-7

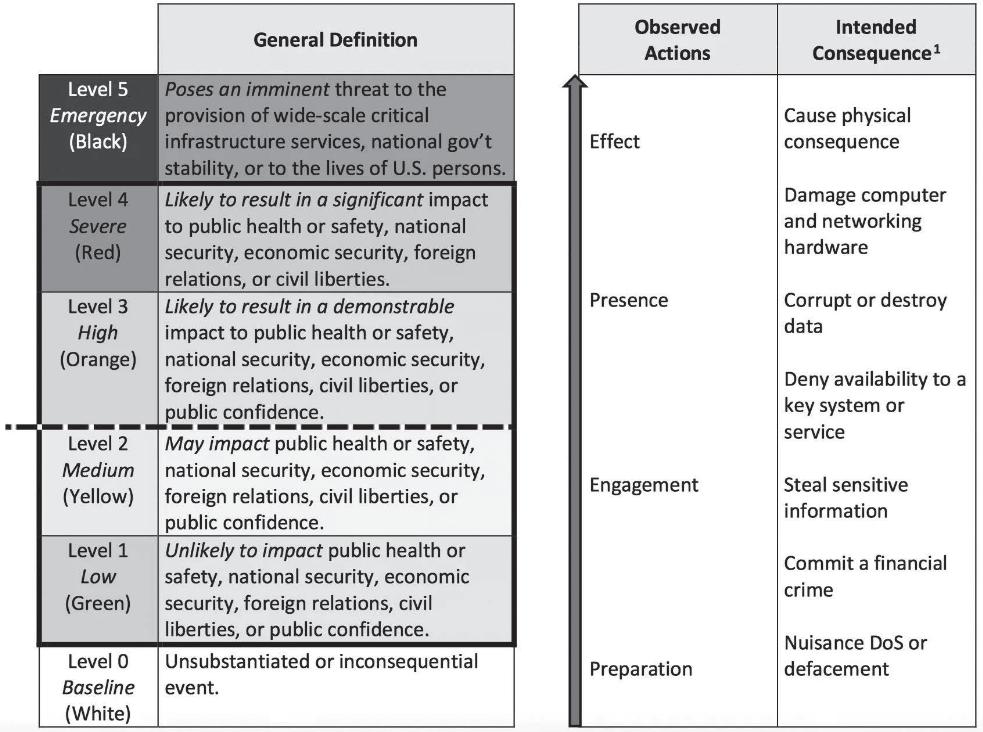
[12] Presidential Policy Directive 21 (PPD–21) on Critical Infrastructure Security and Resilience identifies 16 critical infrastructure sectors: chemical, commercial facilities, communications, critical manufacturing, dams, defence industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste, transportation systems, and water and wastewater systems.

[13] *Legend:* WH = White House; NSC = National Security Council; ODNI = Office of the Director of the National Intelligence; DoD = Department of Defense; DoS = Department of State; DHS = Department of Homeland Security; DoE = Department of Energy; DoC = Department of Commerce; DoJ = Department of Justice.

First, the underlying dilemma starts at the issue of what are the thresholds for government-level response. The methodology for assessing the effect of a cyberattack campaign, and calculating an unacceptable level of “damage” after which the critical cyberattack threshold will be crossed is still evolving. The federal government is primarily responsible for its own governmental networks. Beyond that, it takes first-order responsibility for national security level threats that constitute a *significant cybersecurity incident* in the official parlance. The notion of a major cybersecurity incident was first determined in a memo for the federal agencies by the Office of Management and Budget in 2007. OMB is the largest office within the Executive Office of the President, and it issues the Federal Information Security Management Act guidance, the key point of reference for homeland security planning. The guidance of 2014, based on U.S. CERT National Cyber Incident Scoring System defines *incident* as “an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.” An updated version of 2015 defines a *major incident* as one that:

- Involves information that is classified or “controlled unclassified information”, a broader category that includes proprietary information, intellectual property, trade secrets or personally identifiable information.
- Affects at least 10,000 users and is not “recoverable” (for example, sensitive data is exfiltrated from agency systems and publicly posted online. Or, the time to recover is unpredictable or would require additional resources.)
- Causes an agency to lose the ability to provide a critical service to at least some users. A “high-functional” impact, meanwhile, describes an incident in which an agency loses the ability to provide *all* critical services to users.
- Involves the exfiltration, modification, deletion or any other type of unauthorized access of information or system. [14]

There are seven levels of severity based on the impact caused and the recoverability and dependency of the systems affected. The Obama presidency got one step closer to categorizing the national security levels of cyber incidents in the U.S. Cyber Incident Coordination presidential directive issued on 26th July 2016. It also uses the same terminology and scoring system. Under the directive, all major incidents that is those in the top three categories are also considered “*significant cyber incidents*, meaning they are likely to result in *demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties or public health and safety of the American people.* These significant cyber incidents demand unity of effort within the Federal Government and especially close coordination between the public and private sectors as appropriate.” [15] Another factor seems to influence governmental intervention, when the attacker is verifiably a nation state. Obama regularly refers to this as a pivotal part of the calculation. In that case, international law kicks in as the regulatory norm. The next chapter examines international law considerations.



	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

Observed Actions	Intended Consequence[1]
Effect	Cause physical consequence
	Damage computer and networking hardware
Presence	Corrupt or destroy data
	Deny availability to a key system or service
Engagement	Steal sensitive information
	Commit a financial crime
Preparation	Nuisance DoS or defacement

Figure 2. *Incident scoring in the PPD–41 Presidential Policy Directive “United States Cyber Incident Coordination”.* [20]

According to these measures, the 2016 Russian hacking meets the standard for a significant cyber incident, as there has been demonstrable impact to public confidence and foreign relations.

Secondly, it is blurred to what extent cybersecurity is a civilian or a military responsibility. Currently, cyberattack response is predominantly a civilian law enforcement, counterintelligence and incident response procedure, combined with a (voluntary) regulatory framework serving defence and resilience[14] purposes. In baseline terms, the Department of Homeland Security is responsible for the dot.gov cybersecurity and the public-private partnership with critical infrastructure stakeholders. Meanwhile, the information security technical expertise in the civilian sector is split between the Department of Homeland Security where the US–CERT resides, and the Department of Commerce through the mandate of the National Institute of Technology that is authorized to elaborate voluntary cybersecurity frameworks.

[14] In generic terms resilience is the ability to quickly restore the original shape after an attack. It is an integral part of Information and Communication Technology security incident management and homeland security. Fast recovery limits potential gains and can convince an opponent not to attack.

The U.S. Cyber Incident Coordination presidential directive issued on 26th July 2016 institutionalizes a whole-of-government approach: the directive designates the Department of Justice, acting through the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force, as a lead agency in charge of responding to cyber threats, meaning investigation and prosecution, against the United States agencies or companies. When cyber incidents occur, the Department of Homeland Security provides assistance to potentially impacted entities, analyses the potential impact across critical infrastructure, investigates those responsible in conjunction with law enforcement partners, and coordinates the national response to significant cyber incidents. [16]

At the level of industry, during a real-world attack on the grid, the Department of Energy would be responsible for collecting, evaluating, and sharing information on our energy infrastructure, as well as working with Federal, state, and local entities and industry to help facilitate the restoration of damaged energy infrastructure. (DARPA is interested specifically in an early warning of impending attacks, situation awareness, network isolation and threat characterization.)

The Director of National Intelligence (DNI) assists in aggregating analysis of threat trends, and helps "to degrade or mitigate adversary threat capabilities". [16] The Department of State can reach out through diplomatic channels directly to foreign governments where the source of the attack is located. In the aftermath of the Sony attack, on 1 April 2015 Obama issued an executive order entitled *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.* The Treasury has the authority to levy sanctions against those charged with cyber felony receiving advice from the Department of Commerce and the Office of the U.S. Trade Representative.

Since the 1980s and increasingly from the early 2000s the FBI, endowed both with counterintelligence and law enforcement authorities, has been the lead federal agency for investigating cybersecurity incidents. During the Obama Administration, the cybersecurity remit of the Department of Justice (DoJ) has been extended considerably. John Carlin the head of the DoJ's National Security Division said the coordinated national security investigative and prosecution process and all source intelligence and attribution capability within the DoJ is essential, and these are pieces of a new deterrence strategy. Carlin described the national security investigations procedure—that was established in reaction to 9/11 attacks through the USA PATRIOT Improvement and Reauthorization Act—that it: "seek to harness and coordinate the authorities and capabilities of all members of the national security community, state and local law enforcement, and foreign law enforcement and intelligence partners, and may result in a wide variety of national security activity, including […] arrest and prosecution of perpetrators, imposition of economic sanctions, diplomatic overtures to foreign governments, and actions undertaken by U.S. intelligence services or armed forces overseas." [17]

DoJ is responsible for both national security and cyber economic espionage investigations, attribution and prosecution. Carlin also linked their task to the globally promoted U.S. norms on acceptable behaviour in cyberspace which are enforced by this cross-border law enforcement procedure.

DoD's Role in Cyber Defence

The public debate about the role of the Department of Defense in national cybersecurity has been ongoing for more than a decade. There are signs on the part of the legislative and executive authorities to be inclined to delegate more role to the military. Along with the extended scope of the DoJ and international norms discussed in the next chapter, the military constitutes the other major source of deterrence. When the 2011 DoD Strategy for operation in Cyberspace was issued, the DoD was only responsible for the cybersecurity of the dot.mil domain. As set by domestic law, the military can only provide *assistance* to domestic civilian authorities in special cases related, for example, to counterterrorism, WMD or cybersecurity. DoD has developed and issued key *Defense Support of Civil Authorities,* however, DoD guidance does not clarify the specific roles and responsibilities of key DoD entities that may be demanded to support a cyber incident.

There has been a considerable change in the DoD's role conception after 2012, when in August Saudi Aramco was smashed by a massive cyberattack, and later in September several Wall Street banks were also hit by a series of DDoS attacks for over a week, and the attacks stopped completely only in spring 2013. Since then, a more direct role is articulated for the military in critical infrastructure protection. As of today, the military is also involved in civilian cybersecurity exercises and also in strategic planning, most notably in the yearly Cyber Guard exercises that has shifted from a whole-of-government to a whole-of-nation approach. In the 2015 DoD Cyber Strategy it is one of the five strategic objectives to "be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyber-attacks of significant consequence". [18: 14] The Strategy also identifies a role for the four groups of mission forces of which the 13 "National Mission Forces and their associated support teams will defend the United States and its interests against cyberattacks of significant consequence", thus, they will help defend the nation's critical infrastructure. [18: 6] Unambiguously, the DoD possess the highest level of aggregate cybersecurity expertise both in qualitative and quantitative terms. In the U.S., however, there is a statutory restriction, the so-called Posse Comitatus Act, concerning the employment of the military force on the homeland in peacetime. Rather, it is the National Guards who can operate more freely at local levels, and who will have a major role in cyber defence if it is necessitated. Most national security strategic documents determine this as the last resort.

In December 2015 the White House Strategy on Cyber Deterrence was delivered. It had been commissioned in 2013 by Congress in the *National Defense Authorization Act*, with the purpose of outlining how the United States will respond to cyberattacks. It came out almost two years late, and between April and December 2015 informally the DoD strategy was regarded as a kind of interim national cybersecurity strategy. Another strategic ambition running parallel to national cybersecurity is the full integration of cyber capabilities into military operations and deterrence. Cyber Command have been boosted to more than 6,000 troops and cybersecurity budgets, although precise chapters are indiscernible, have multiplied. In the military strategic context, designated cyber troops are intensively building technical, tactical and C2 operational skills. Rules of Engagement are still in progress, and they are largely classified. In 2016, the DoD launched a task force to explore ways, in which offensive cyber capabilities could provide support to strategic objectives with results to be expected when cyber forces become fully operational. Its mandate is to find ways to operationalize offensive operations: "[T]he role of full-spectrum cyberspace operations in supporting shaping, deterrence, constrained military objectives, and full-scale conflict is not adequately appreciated or understood. It is the principal objective of this TF to investigate the opportunities for, and limitations of, offensive cyber capabilities in support of overall U.S. strategy and provide actionable recommendations to enhance those capabilities." [19: 32]

The Delicate Balance of Public-Private Partnership

Third, the division of labour between the federal government and private sector actors in cybersecurity is still unsettled. Both parties are still hesitant about the degree of responsibility they are willing and able to take for cybersecurity. The executive branch and private sector relationships are entangled but crucial in any sincere cybersecurity efforts. One of the first and best known exercises examining the issue of strategic information warfare was the 1996 RAND "The Day After" desktop exercise and the following report characterizes the federal government's role as part leadership and part partnership with the domestic sector. Similarly, President Obama and leading DHS cybersecurity officials emphasize that in private sector cybersecurity the government has only an enabling role, providing the private sector with the necessary guidance, early warning and information, incident management assistance and incentives to assist in risk management. In the federal government's discourse, cyberspace is an ecosystem with shared responsibilities. As an initial overture in 2011, the White House submitted a comprehensive cybersecurity proposal to Congress including obligatory cybersecurity standards and voluntary cybersecurity practices that could be required to be adopted by critical infrastructure owners, but it was rejected as a result of the powerful industrial lobby. It was a stark reminder that progress in this area is not just a technical regulatory issue, but rather a tough bargain. Later on, the President submitted several regulatory bills, but there has been little change in the basic stance of the industry's voluntary stance.

In 2016, during the Presidential Commission on Enhancing National Cybersecurity hearings, possible further solutions were gauged along the regulatory versus voluntary approach and the proactive prevention versus mitigation axles. One enabling policy is fostering information sharing between the private sector and public authorities, while ensuring liability protection and incentives. Despite several bills, confidence is still lacking towards federal agencies. The DNC preventing the FBI from having access to party servers is a good example. Extending the DoJ's investigatory and prosecutorial role was welcome by the business community, unlike the White House's Deterrence Strategy which was criticized for ignoring threats below the level of a significant cyber incident. Following in the footsteps of the 2013 NSA leak, the 2016 NSA hack and leak revealed exploit kits used by NSA to penetrate major IT vendors' products like Cisco or Fortinet, was another blow to the confidence of the private sector towards the government.

The Russian meddling and the increasing number of attacks prove to be a double-edged tactic. The distance between public and private actor views and interests seem to diminish. In this regard, there has been an important shift in the position of the government on the private actors' right to execute (active) defensive measures, even if not on hack backing back. This is a sign of opening up to the idea that the private sector has a major share in cyber power.

In May 2015, the Assistant Attorney General Leslie Caldwell announced plans for a guidance for industry on cyber defensive actions. Up until now, this has not materialized. The demand to legalize forms of self-help for the private industry is increasing. Business leaders and the U.S. Chamber of Commerce also put growing pressure on the administration to expand deterrence to cyber threats that do not rise to the level of warfare, but still cause considerable losses.

Conclusion

The article provides a snapshot of the regulatory and institutional environment of the U.S. cybersecurity back in 2016. U.S. cybersecurity as a national security issue area emerged gradually since the early 1990s, and later on, it was fully elevated to the highest level of strategic planning by the Obama presidency. In spite of supposedly having the most powerful cyber weapon arsenal, the U.S. strategic advantage in cyberspace is greatly diminished by the lack of a coherent and functioning cybersecurity policy. The U.S. is far not alone with this deficiency, however, this calls into serious doubt the ability and willingness of the state supposedly with the most powerful cyber capabilities.

Among the most serious problems, governance remains disjoint and weak all along the statutory, regulatory and enforcement levels. Efficiency would require a shift towards centralization and enforcement of regulations at the federal level, but the presidential orders and legislative acts do not go beyond the voluntary regulation for the private sector. Cyber defence of the federal departments and agencies is also still weak as the Office of Personal Management hack shows. On the other hand, there is some progress in the national incident response management plan and in the whole-of-the nation cyber exercises. Although there is some development towards a bigger role for the military, response mechanism short of war remains largely civilian.

References

[1] Promises about Homeland Security on "The Obameter". *Politifact.com* (online), www.politifact.com/truth-o-meter/promises/obameter/subjects/homeland-security/ (Downloaded: 03.02.2016)

[2] *Joint Publication 1–02. Dictionary of Military and Associated Terms.* Washington, D.C.: Department of Defense, 2007. https://marineparents.com/downloads/dod-terms.pdf (Downloaded: 03.02.2016)

[3] GRAY, C. S.: *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling.* Carlisle, Pennsylvania: Army War College Carlisle Barracks, Strategic Studies Institute, 2007.

[4] WIRTZ, J. J.: Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy. In. GEERS, K. (Ed.): *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications, 2015.

[5] KOFMAN, M.: The ABCs of Russian Military Power: A Primer for the New Administration. *The National Interest* (online), 2 February 2017. http://nationalinterest.org/feature/the-abcs-russian-military-power-primer-the-new-19299?page=5) (Downloaded: 03.02.2016)

[6] OWENS, W. A., KENNETH, W. D., LIN, H. S.: *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington, D.C.: National Research Council of the National Academies. The National Academies Press, 2009.

[7] LIBICKI, M. C.: *Conquest in Cyberspace: National Security and Information Warfare.* New York: Cambridge University Press, 2007. https://doi.org/10.7249/CB407

[8] NYE, J. S. Jr.: *Cyber power.* Cambridge, Massachusetts: Belfer Center for Science and International Affairs. Harvard Kennedy School, 2010.

[9] YARGIN, H. R.: Strategic *Theory for the 21st Century: The Little Book on Big Strategy. U.S. Army War College Strategic Theory.* Carlisle: Army War College Carlisle Barracks, Strategic Studies Institute, 2006.

[10] FREEDMAN, L.: *Strategy: A History.* New York: Oxford University Press, 2013.

[11] CRAIG, T., VALERIANO B.: *How to Think about a State's Cyber Capabilities.* New York: Council on Foreign Relations, 2016. www.cfr.org/blog/how-think-about-states-cyber-capabilities (Downloaded: 20.12.2016)

[12] *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government.* Executive Office of the President, 2015. NIST Computer Security Resource Center (online). https://csrc.nist.gov/Topics/Laws-and-Regulations/executive-documents/CSIP (Downloaded: 20.12.2016)

[13] STERNSTEIN, A.: If hackers cause a blackout, what happens next? *Christian Science Monitor* (online), 2016. www.csmonitor.com/World/Passcode/2016/1116/If-hackers-cause-a-blackout-what-happens-next (Downloaded: 20.12.2016)

[14] *US-CERT National Cyber Incident Scoring System.* www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System (Downloaded: 20.12.2016)

[15] *US-CERT Federal notification guidelines.* www.us-cert.gov/incident-notification-guidelines#impact-and-severity-assessment (Downloaded: 20.12.2016)

[16] *Cyber Incident Response.* Washington, D.C.: Department of Homeland Security, s.d. www.dhs.gov/cyber-incident-response (Downloaded: 20.12.2016)

[17] CARLIN, J. P. (2016): Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats. *Harvard National Security Journal*, 7 (2016), 392–436.

[18] *Cyber Strategy.* Washington, D.C.: Department of Defense, 2015. www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (Downloaded: 20.12.2016)

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

[20] *Presidential Policy Directive – United States Cyber Incident Coordination.* Washington, D.C.: The White House, Office of the Press Secretary, 2016.

[21] *Cybersecurity Office, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* Washington, D.C.: White House, 2009.