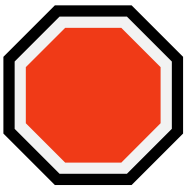
WILLIAM J. PERRY CENTER FOR HEMISPHERIC DEFENSE STUDIES

INSTRUCTIONS FOR THE ONLINE APPLICATION FORM

CYBER POLICY DEVELOPMENT (SPANISH)
(CYBER-S 2021)

Application Period: 04 April – 03 Nay, 2021

Preparatory Phase: 28 June – 09 July, 2021
Active Phase: 19 – 23 July, 2021



WHO CAN USE THIS FORM TO APPLY

- Civilians (government and non-government)
- Retired military
- Non-military police
- Active duty military who live in the Washington, DC metropolitan area.

WE WILL NOT ACCEPT APPLICATIONS DIRECTLY FROM ACTIVE DUTY MILITARY PERSONNEL WHO LIVE OUTSIDE OF WASHINGTON, DC. THOSE INDIVIDUALS MUST CONTACT THE OFFICE OF MILITARY COOPERATION (MILGROUP) AT THE UNITED STATES EMBASSY IN THEIR COUNTRY TO APPLY.

For specific information, please contact our registrar's office at chdsregistrar@ndu.edu

---

Please follow all of the instructions on these pages, as well as those located online on our web page at **http://williamjperrycenter.org/academics**, which contains additional information not found on this here, including the Academic Integrity and Non-Attribution statement, which you agree to abide by if selected for the course.

Once you begin filling out the online application form, you will have to submit it in the same session. You will not be able to save your progress and return to it later.

The application process includes answering some essay questions, located on the online form. The questions specific to this course are listed in section 6. Before loading the application form, you might wish to review the essay questions beforehand and write your responses separately. The online application form will let you copy and paste text into the appropriate text boxes.

The application form is located at the following URL:

https://www.dscarc.org/default?regcenterid=11&eventid=57172&reltype=12479

Please keep in mind that the Perry Center shares this application system with other regional centers; therefore the form is initially presented to you in English. In the upper left-hand side of the page, there is a drop-down menu for automatic translation into various languages. This is designed to help you better understand the application form, but please keep in mind that machine translation is not perfect.

4

After you complete the online application form and have received your confirmation number, please send the following document to **chdsregistrar@ndu.edu**:

- Professional Experience Form (available for download on the course description page)

When you send your documents via e-mail, the subject line must contain your last name, country, course, and confirmation code provided to you by the system. *Failure to provide this information with your documentation may result in delays processing your application.*

Example: **SMITH – JAMAICA – CYBER-S 2021 – QPLFHNJ1234**.

Please ensure that the combined total file size of your attachments does not exceed 8 MB. We will not grant deadline extensions due to messages being rejected by our e-mail server.

Applications will not be considered complete until the Perry Center receives all of the required documents (Online application form, Professional Experience Form)

5

Upon submitting an application, you certify that you:

- Have read the general course description, candidate profile, and the application instructions on this document and web site.
- Understand these instructions and agree to abide by the National Defense University's Academic Integrity Policy.
- Understand that all courses are subject to availability of funds.
- Meet the language requirements for this course, and (if selected to participate or placed on the waiting list) will take an English reading comprehension exam (if asked).
- All information you have provided is accurate.

All applicants will receive notification via e-mail approximately ten weeks before the start of the course if they have 1) been selected, 2) have been placed on the waiting list, or 3) have not been selected.

6

ESSAY QUESTIONS

1. Please describe in detail your current job duties and work activities in relation to cybersecurity at the policy and strategic level. (200 word max)

2. Please describe your organization's mission (at the policy/strategy level) in relation to cybersecurity and/or defense. (200 word max)

3. Please describe how this course will help you personally (now or in the future), or your organization, to develop a policy (and/or strategy) for cybersecurity. (200 word max)

4. After reading the attached article, what is your opinion of its application at policy and strategy level. (200 word max)

Evolution of US Cybersecurity Strategy

Saltuk Karahan[1], Hongyi Wu[2] and Leigh Armistead[3]
[1]Department of Political Science and Geography, Old Dominion University, Norfolk, USA
[2]Department of Electrical and Computer Engineering, Old Dominion University, Norfolk, USA
[3]Peregrine Technical Solutions, LLC, USA
skarahan@odu.edu
h1wu@odu.edu
larmistead@gbpts.com

Abstract: This paper explores the evolution of the overall Cybersecurity Strategy of the United States, analyzing the change in focus as well as effects of events and technology in this change. It examines the National Security Strategy documents and how cybersecurity is handled in these documents, making further analysis of specific cybersecurity documents by several departments in the U.S. administration within the last decade. From this research, it was determined that the overall cybersecurity strategy is shaped by involvement of several stakeholders along with security perspectives of different administrations, thereof how cybersecurity strategies have changed, and are reflected in the cybersecurity strategies of the different departments and agencies. Specifically three factors with their relevant influence in the evolution of approach to national cybersecurity strategy are further analyzed with their respective influences, to include (1) international relations within the framework of global security, (2) specific incidents of cybersecurity in this period and (3) innovation and technology. While each of these factors had an effect in the shaping of the overall U.S. Cybersecurity Strategy documents, the focus of analysis is on "to what extent each of these factors was reflected in the strategy documents and the scope of their influence" is of utmost importance. It is our opinion that an analysis of the focus shift and the reflection of the prominent factors into the strategy documents will benefit shaping new strategy documents as well as raising awareness about the mindset behind these documents. The findings of this study indicate an increasing influence of global security environment and innovative approaches in strategy documents, as a consequence of comprehensive perspective and increasing level of expertise in cybersecurity.

Keywords: cybersecurity, strategy, national security, U.S. security strategy

1. Introduction

As the discipline of cybersecurity evolves by time, so do the strategies developed by specific agencies or departments within nations (Tatar et.al. 2014). We have evaluated a number of U.S. strategy documents within the last ten years, have focused in how these documents changed by determining and qualitatively analyzing the factors behind these changes. Using a content analysis methodology, this paper first determined the three factors predominantly influencing the change in strategy, to include (1) international relations within the framework of global security, (2) specific incidents of cybersecurity in this period and (3) innovation and technology. Overall this paper is organized in five sections, with the introduction stating the rationale for the research, methodology and the organization of the paper. In the second section, ten different documents in five groups within the last 10 years from several agencies are described in the way they approached to cybersecurity along with their commonalities with and differences from other strategy documents. The third section outlines the main factors influencing the change in strategy and describes how each factor's influence is seen in the documents. The fourth section analyzes these factors with their relative influence, makes comparisons and presents the findings on their level of influence. Finally, the last section draws conclusions from the findings and proposes a research agenda on the study of national cybersecurity strategy.

2. Background

We have analyzed the recent cybersecurity strategy documents in 5 main groups. The first group is comprised of National Security Documents which included parts about cybersecurity strategy. The second and third group include department level cybersecurity strategy documents (DoD and DHS respectively). The fourth group includes the two presidential cybersecurity strategy documents and the fifth group is the Presidential executive orders related to cybersecurity.

2.1 Recent documents of cybersecurity strategy in the U.S.

1)U.S. National Security Strategies (2010,2015,2017): Although National Security Strategies are not solely focused on cybersecurity, all National Security Strategy documents within the last 10 years specified the

criticality of cybersecurity in National Security. Two of the National Security Strategy (NSS) documents within the last 10 years were those signed by President Obama and the last one is the one signed by President Trump.

Apart from the overview and conclusion, 2010 NSS lists two sections of "Strategic Approach" and "Advancing our Interests". Under the section "Advancing Our Interests", subsections of Security, Prosperity, Values and International Order are listed. Under the title of "Secure Cyberspace", almost a full page of the 10-page long security subsection lists two main action items as Investing in People and Technology, Strengthening Partnerships. In the subsection of "Prosperity", cybersecurity is mentioned with respect to cybercrime, global commons and Asian allies.

In 2015 NSS, very similar to the 2010 NSS, Security, Prosperity, Values and International Order are the main sections. Strategic Approach is defined in the introduction. A larger portion is dedicated to Cybersecurity with regard to Assuring Access to Shared Spaces (global commons argument). A commitment to assist other countries to develop laws that enable strong action and the requirement for long-standing norms of international behavior is mentioned. Unlike the document in 2010, there is country specific cyber threat definition in the 2015 document. In the section "Advancing Our Rebalance to Asia and the Pacific", China is mentioned with cyber-theft.

The 2017 NSS was prepared by an administration having a different view on national security and was comprised of four pillars and a strategy on regional context. The four pillars are:

- (1) Protect the American People, the Homeland, and the American Way of Life,
- (2) Promote American Prosperity,
- (3) Preserve Peace through Strength,
- (4) Advance American Influence.

As in the previous two NSS documents, under Pillar I (Protect the American People, the Homeland, and the American Way of Life) which is focused on Security, one and a half page is dedicated to Cybersecurity under the section "Keep America Safe in the Cyber Era". This latest NSS lists priority actions as

- (1) Identify and Prioritize Risk,
- (2) Build Defensible Government Networks,
- (3) Deter and Disrupt Malicious Cyber Actors,
- (4) Improve Information Sharing and Sensing,
- (5) Deploy Layered Defenses.

In addition to the coverage of cybersecurity in Pillar I, Pillar II (Preserve Peace through Strength) also dedicates a subsection to Cyberspace under the section Capabilities. The use of cyberspace by malicious state and non-state actors for "extortion, information warfare and disinformation" is mentioned along with the capability of these attacks in "undermining faith and confidence in democratic institutions and the global economic system". Furthermore, similar to the nations like Russia and China who approach cybersecurity in the broader context of information warfare, under the section "Diplomacy and Statecraft", a sub-section is dedicated to "Information Statecraft" focusing on the use of cyberspace in diplomacy and statecraft.

2) U.S. Department of Defense (DoD) Cyber Strategies (2011,2015): At the forefront of Cyber War, DoD has been one of the main actors – if not the main actor – in shaping U.S. Cybersecurity Strategy. The two documents analyzed for this paper were "Department of Defense Strategy for Operating in Cyberspace (July 2011) and "The Department of Defense Cyber Strategy (April 2015)".

Department of Defense Strategy for Operating in Cyberspace (July 2011) lists five strategic initiatives for defense in cyberspace:

- (1) Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential,

- (2) Employ new defense operating concepts to protect DoD networks and systems,
- (3) Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy,
- (4) Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity
- (5) Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

Four years later, another DoD document, The Department of Defense Cyber Strategy (April 2015), employed a similar method in defining strategy and listed five strategic goals along with implementation objectives related to each strategic goal. The five strategic goals in this document are:

- (1) Build and maintain ready forces and capabilities to conduct cyberspace operations;
- (2) Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions;
- (3) Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence;
- (4) Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages;
- (5) Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability. As partnership with other government departments became natural, it was not listed among strategic goals and the focus was moved to "building and maintaining viable options against conflicts" which implied resilience and recovery planning.

Overall, the change in DoD cybersecurity strategy was indicative of an increasing maturity of understanding cybersecurity. In the earlier strategy documents, the mindset was changed by recognizing cyberspace as an operational domain, whole of government approach was adopted and alliance building was advocated. The action items for the strategy were focused on technological innovation and workforce development. In 2015, in addition to the specific strategic goals, how to reach these goals were further elaborated with "implementation objectives". Likewise, specific nation states (Russia, North Korea, Iran and China) were mentioned in the document with their respective threat postures.

3) U.S. Department of Homeland Security (DHS) Cybersecurity Strategy (2018): Although DHS has the responsibility and legal authority in securing cyberspace, it has been short of human capital to develop a cybersecurity strategy for several years. DHS released DHS Cybersecurity Strategy document in 2018 and the document brought a risk management approach with more technicality in its procedural approach compared to the previous strategy documents. The technical innovations in attacks are reflected in the threat assessment section of the document. In its threat description, the DHS strategy has more references to the emerging technological/methodological changes like ransomware, darkweb and the use of cryptocurrencies. The document lists five pillars and seven associated goals:

- Pillar I – Risk Identification
- Goal 1: Assess Evolving Cybersecurity Risks. We will understand the evolving national cybersecurity risk posture to inform and prioritize risk management activities.);
- Pillar II – Vulnerability Reduction
- Goal 2: Protect Federal Government Information Systems. We will reduce vulnerabilities of federal agencies to ensure they achieve an adequate level of cybersecurity
- Goal 3: Protect Critical Infrastructure. We will partner with key stakeholders to ensure that national cybersecurity risks are adequately managed.);
- Pillar III – Threat Reduction

- Goal 4: Prevent and Disrupt Criminal Use of Cyberspace. We will reduce cyber threats by countering transnational criminal organizations and sophisticated cyber criminals.);
- Pillar IV – Consequence Mitigation
- Goal 5: Respond Effectively to Cyber Incidents. We will minimize consequences from potentially significant cyber incidents through coordinated community-wide response efforts.);
- Pillar V – Enable Cybersecurity Outcomes
- Goal 6: Strengthen the Security and Reliability of the Cyber Ecosystem. We will support policies and activities that enable improved global cybersecurity risk management
- Goal 7: Improve Management of DHS Cybersecurity Activities. We will execute our departmental cybersecurity efforts in an integrated and prioritized way.)

DHS Cybersecurity Strategy also lists seven guiding principles that form a basis in the alignment of the departmental activities. These principles are:

- 1. Risk prioritization.
- 2. Cost-effectiveness.
- 3. Innovation and agility.
- 4. Collaboration.
- 5. Global approach.
- 6. Balanced equities.
- 7. National values.

In its context, DHS Cybersecurity Strategy defines a series of objectives and sub-objectives for each goal as the action items of the strategy. In addition to the risk management approach as a procedural development, emerging technologies are referenced more often in the DHS Cybersecurity strategy.

4) International Strategy for Cyberspace (2011) and National Cyber Strategy of the U.S.A (2018): The first national cybersecurity document was released in 2003 by the Bush administration, however, this paper considers the most recent next two documents specific to cybersecurity strategy at the national level. As seen in the names of the two documents, an institutionalist approach was embraced in the 2011 document and a rather realist approach was preferred in the latest National Cyber Strategy document in 2018. While International Strategy for Cyberspace (2011) never mentions any adversarial state, National Cyber Strategy of the U.S.A (2018) mentions Russia, China, Iran and North Korea with their respective challenges to American cybersecurity. A comparison of the National Cyber Strategy (2018) to its predecessor, The National Strategy to Secure Cyberspace (2003), also indicates the changing global emphasis. National Cyber Strategy of the U.S.A (2018) states that "The articulation of the National Cyber Strategy is organized according to the pillars of the National Security Strategy." In 2003, although it was drafted by a hawkish administration with global ambitions, the strategy was organized "Consistent with the objectives of the National Strategy for Homeland Security," This also is an indicator that global emphasis on the cybersecurity documents has increased and nation states are rather seen as the sources of threat. It should be noted that the shift from a unipolar world to a multipolar world can also be a reason for this. In 2003, the U.S. was still seen as unchallenged actor in the international arena and threat perceptions were mostly based on global terrorism rather than rival / nuisance states and this general concern was reflected in its approach to national security.

5) Presidential Executive Orders (2016, 2017): In addition to the strategy documents, two presidential orders were signed by President Obama and President Trump with just fifteen-month gap. These two documents rather reflect the organizational mindset difference between the two administrations. While President Obama's Executive Order attempts to establish a commission and approach to the problem in a rather centralized manner, President Trump's Executive Order states the accountabilities of the departments and tasks them with

developing plans having tight deadlines and employs Presidential Special Advisors for the approval of the plans. President Trump's Executive order has a hierarchical centralization more than a functional centralization. The security in cyberspace is given to each department/agency as a responsibility and the central control mechanism is the President's office for these tasks. In President Obama's Executive order, a central mechanism specific to the subject of cybersecurity is envisioned and different agencies/departments are represented in this central mechanism.

2.2 Change of focus in U.S. cybersecurity strategy

From the content of the strategy documents released since 2010, several inferences can be made about the shift in focus related to matters of cybersecurity. Below are the general observations made by a contextual analysis of the cybersecurity strategy documents examined above:

- Nation state involvement is emphasized strongly and cybersecurity is more likely to be seen as part of broader national security and it has gained more global emphasis.
- As our understanding of cybersecurity has developed, new conceptual approaches like risk management, reference to the emerging technologies (in terms of threats they enable) are seen more often in the documents.
- National Security approaches of the administrations are clearly seen. However, despite the differing threat understanding between the two political parties (Democrats focusing on Russia and Republicans focusing on China in general matters of international security), in the cybersecurity realm, both Russia and China are explicitly seen as threats.
- Despite the commonality in general tendency like seeing cybersecurity as a component of broader international security and increasing references to the emerging threats, department/agency specific contents still exist (White House, DoD and DHS still see cybersecurity from their own perspectives).
- Regardless of different administrations' general threat assessments in the international security environment, approach to the governance of national cybersecurity is different in the temporally close two White House executive orders. However, this difference can be seen as a change specific to the organizational mindsets of the respective administrations rather than an evolution in cyberspace.

3. Factors influencing the change in strategy

We identified 3 factors which has an influence on cybersecurity strategies using the context analysis methodology. These factors are international security environment, cyber incidents and technological developments. In the later part of this section these three factors are explored with their respective influence.

3.1 International security environment

There has been significant change in the international security environment since 2010. The DoD assessment in 2018 acknowledges this change and lists Russia, China, North Korea and Iran as the states attempting to expand their influence in a strategic competition. (DoD, 2018) Specifically since late 2013, a shift has been observed in the international security environment and this has been seen as a transition from the post-Cold War era to a renewed great power competition along with challenges to U.S. led international era that existed for several decades (O'Rourke, 2016). Based on the observations from several prominent scholars, the Congressional report drafted by R. O'Rourke lists emerging characteristics of the new international security situation as: "

- Renewed ideological competition, this time against 21st-century forms of authoritarianism and illiberal democracy in Russia, China, and other countries;
- The promotion by China and Russia through their state-controlled media of nationalistic historical narratives emphasizing assertions of prior humiliation or victimization by Western powers, and the use of those narratives to support revanchist or irredentist foreign policy aims;
- The use by Russia and China of new forms of aggressive or assertive military, paramilitary, information, and cyber operations—called hybrid warfare or ambiguous warfare, among other terms, in the case of Russia's actions, and salami-slicing tactics or gray-zone warfare, among other terms, in the case of China's actions;

- Challenges by Russia and China to key elements of the U.S.-led international order, including the principle that force or threat of force should not be used as a routine or first-resort measure for settling disputes between countries, and the principle of freedom of the seas (i.e., that the world's oceans are to be treated as an international commons); and
- Additional features alongside those listed above, including
- Continued regional security challenges from countries such as Iran and North Korea;
- A continued focus (at least from a U.S. perspective) on countering transnational terrorist organizations that have emerged as significant nonstate actors (now including the Islamic State organization, among other groups); and
- Weak or failed states, and resulting weakly governed or ungoverned areas that can contribute to the emergence of (or serve as base areas or sanctuaries for) nonstate actors, and become potential locations of intervention by stronger states, including major powers." (O'Rourke, 2016).

When the cybersecurity strategy documents are analyzed with this shift in the overall international security environments, it is seen that not surprisingly, this shift is more reflected in the DoD documents with specific mentioning of China, Russia, Iran and North Korea. Apart from the existing relationships, the international security approach of the administrations are reflected in these documents (there is more idealistic focus on cooperation in the documents during Obama administration). In the earlier versions, cybersecurity strategies were not explicitly linked to the international security. This also stemmed from the vagueness of the threat environment (attribution problem in cybersecurity) and the post-Cold War security mindset which focuses on capability development rather than a specific notion of "enemy" or threat. However, as the international security environment evolved into a state level competition and challenge, the weight of this factor has increased by time. However, as the nation states' threat in cyberspace recognized the relative weight of the link between cyberspace and terrorism lost it significance. In the 2010 NSS document the terrorist threat in cyber space was explicitly stated, this emphasis was lost in the following NSS documents of 2015 and 2017. This threat was more strongly expressed in DHS and DoD Cybersecurity Strategy documents.

3.2 Cyber incidents

In the non-transparent world of cybersecurity, the cyber incidents have been the factors predominantly and implicitly shaping the discourse in the strategy documents. It is natural that as cyber incidents threatening national security were discovered, they helped the strategy drafters understand the nature of existing threats and consequently these definitions were expressed in the documents. Council on Foreign Relations has been tracking the cyber incidents that have occurred since 2005 and publish an extensive list of these incidents. Their latest findings list twenty countries suspected of sponsoring cyber operations and emphasize that "states have occasionally used cyber operations to cause power outages, as Russia is suspected to have done in Ukraine in 2015 and 2016" (Cyber Operations Tracker, 2018). Although the use of sanctions and punitive actions have been rising according to the report by CFR (Cyber Operations Tracker, 2018), there has not been an increase in the reference to the cyber incidents in the making of strategy documents. It can be observed that cyber incidents have been used to define the threat environment in the earlier documents, however they are referred less in recent strategy documents. It can be argued that the overuse of cyber incidents in strategy documents are indicative of a reactionary view in these documents and will guide the action items focus on the cyber threats similar to those that already occurred.

3.3 Technological developments

Cyberspace has been an area of continuous technological innovation and the strategy documents are expected to keep pace with these innovative changes. We have analyzed both how emerging technologies are reflected in these documents and if there are innovative approaches in securing cyberspace. Rise of dark web, bitcoin, rise of social media, cloud computing, smartphone technology and critical infrastructure were among the emerging technologies which provided cybersecurity challenges with their unique characteristics (Jang-Jaccard and Nepal, 2014). Likewise, risk management approach, concepts of resilience and recovery were among methods gaining prominence in dealing with cybersecurity (Karabacak and Tatar, 2014).

There is a stronger reference to technological innovation and adoption of innovative techniques in recent cybersecurity strategy documents. In the latest National Cybersecurity Strategy, ensuring the government lead in best and innovative practices is listed as an action item and it is stated that: "To protect against the potential threat of quantum computers being able to break modern public key cryptography, the Department of Commerce, through the National Institute of Standards and Technology (NIST), will continue to solicit, evaluate, and standardize quantum-resistant, public key cryptographic algorithms." Investment in next generation infrastructure is also listed as an action item and there are several references to the developments in the field like artificial intelligence and quantum information science. This appears to be a natural result of increasing expertise in the area and improved understanding of the cyber threat environment.

4. Analysis and results

Content analysis has been used as a method to analyze factors influencing the change in U.S. cybersecurity strategy documents and the relative weight of the three factors in this change. The strategy documents are used to define the existing challenges in cybersecurity and guide the capability development, overall preparedness, organizational structures to be established and actions to be taken to meet the challenges. This guidance is eventually expected to be a basis for the resource allocation and responsibilities for several agencies.

The threat environment was defined with the existing cyber incidents that had been experienced and there has been little reference to the underlying technological developments in the earlier strategy documents. In terms of cyber incidents, as events were discovered, they were mentioned in the strategy documents. In 2015, there were references to cyber espionage and theft, and in 2017, after the interference in elections, political subversion was added to the cybersecurity strategy documents.

In the earlier cybersecurity strategy documents, despite the frequent referral to overall technology, there was little specification of the emerging technologies that could pose threat. It is observed that recent documents of strategy put greater emphasis on the emerging technologies and drew attention to their possible use in cybersecurity. In the definition of the threat environment, even with the existing defensive mindset, possibilities due to emerging technologies are not explicitly stated. The use of terminology related to advances in technology in the threat assignment serves as a guidance for the subordinate agencies in which possibilities to consider and how to develop capability for action. Likewise, international security and the threats posed by nation states were not mentioned in the earlier documents of cybersecurity strategy. As the cyber attacks from nation states increased and the sources were revealed, the strategy documents had a higher degree of referring to these threats. The emphasis to global events were naturally seen mostly in the national level strategy documents and in DoD's documents. Unlike many autocratic countries that prefer top secret level secrecy for national strategy documents, these documents are public in many Western countries and nation/state names are stated in such documents. In Western democracies these documents also carry a strategic message to the outside world and are used as means of deterrence. The executive orders analyzed for this paper had little content from the factors influencing strategy and were more focused on the organizational structure to cope with cybersecurity problems (centralized or decentralized approaches are preferred in these documents

Table 1: Influence of factors in U.S. strategy documents (cybersecurity strategy documents or cybersecurity sections in other strategy documents)

Document	Date	Source	International Security	Technology and Innovation	Cyber Incidents
U.S. National Security Strategy	2010	White House	Little emphasis on "potential adversaries"	Not emphasized	Little emphasis on cyber incidents, without specification.
International Strategy for Cyberspace	2011	White House	Emphasis on cooperation and partnership Stability through norms	"Technology" is frequently emphasized, but no specific technology relating to cybersecurity is mentioned	Little emphasis on cyber incidents
DoD Strategy for Operating in Cyberspace	2011	DoD	Reference to international partners Nation states not mentioned	National Cyber Range for emerging technologies New acquisition cycles	Botnets, insider attacks Focus on external threat actors, insider threats, supply chain vulnerabilities, and

Document	Date	Source	International Security	Technology and Innovation	Cyber Incidents
					threats to DoD's operational ability.
U.S. National Security Strategy	2015	White House	Russia and China's cyber attacks are mentioned	Not emphasized	Espionage and attacks are mentioned
DoD Cyber Strategy	2015	DoD	Russia, China, Iran and North Korea are mentioned	Frequent referral to technology, but little specification	N. Korea attack on Sony, China's cyber theft are referred
Presidential Executive Order (Obama)	2016	White House	No referral	Referral to IoT and cloud computing	No referral
Presidential Executive Order (Trump)	2017	White House	No referral	Referral to technology, but no specification	No referral
U.S. National Security Strategy	2017	White House	Russia and China are mentioned	Not emphasized	Political subversion is introduced in the document.
DHS Cybersecurity Strategy	2018	DHS	Little emphasis on the international security.	Risk Management approach Cloud or shared services	General definition of threat, no reference to specific cyber incident
National Cyber Strategy	2018	White House	Russia, China, Iran and North Korea are mentioned	Risk Management Artificial Intelligence Quantum Information Science	China's cyber espionage Data Breaches Ransomware

5. Conclusion

This paper explored the change in U.S. doctrine by analyzing the basic cybersecurity strategy documents within the last ten years. The latest cybersecurity strategy document, Cybersecurity National Strategy (September 2018) states that "The Strategy's success will be realized when cybersecurity vulnerabilities are effectively managed through identification and protection of networks, systems, functions, and data as well as detection of, resilience against, response to, and recovery from incidents; destructive, disruptive, or otherwise destabilizing malicious cyber activities directed against United States interests are reduced or prevented; activity that is contrary to responsible behavior in cyber-space is deterred through the imposition of costs through cyber and non-cyber means; and the United States is positioned to use cyber capabilities to achieve national security objectives." This statement describes the level cybersecurity strategy has reached over time. While in the first sentences the innovative technological or procedural approaches like risk management and resilience are acknowledged, as a result of seeing cybersecurity an inseparable part of national security, the threat in cyberspace is considered as a threat which can be deterred with all means of coercion and cyber power is recognized as a tool of coercion which can be used in all areas of national security.

Increasing aggressions in cyber space is a threat to the Westphalian system of states, where each nation state has sovereignty over its territory and domestic affairs, to the exclusion of all external powers, on the principle of non-interference in another country's domestic affairs (Tatar et.al., 2017). The three factors analyzed in this paper have dominated the strategy documents at an increasing level with increasing focus of international security and technology as a consequence of comprehensive approach and increasing sophistication in our understanding of cybersecurity. A proactive cybersecurity strategy planning requires both global perspective and careful observation of emerging technologies (like the developments in Artificial Intelligence) which will eventually have an effect on cybersecurity. The consideration of emerging technologies instead of focusing on past cyber incident makes the strategy documents more proactive and the consideration of the international security environment brings a comprehensive approach to cybersecurity. The evolution of the strategy encompassing these two aspects is a significant indicator of the need for more interdisciplinary approach to the problem.

The evolution and the change of the strategy documents also raises the question of who should lead U.S. cybersecurity efforts to forefront. The question has been asked earlier and several recommendations have been

provided (Newmeyer, 2012). Another response to this question comes from Tatar et.al. (Tatar et.al., 2016), in which an analytical framework for evaluating the national cybersecurity efforts introduced. While DHS has recently assumed a leadership role, its manpower shortage has been one of the obstacles and increasing international security emphasis maintains DoD's crucial role in national cybersecurity efforts. The governance structure in the two Presidential Executive Orders that were analyzed in this paper provide insights on different approaches to managing national cybersecurity efforts. We believe that this question is still relevant and the changing weight of the factors analyzed in this paper will contribute to the discussions on this question as well.

References

Cyber Operations Tracker (2018). Council on Foreign Relations, Available from: https://www.cfr.org/interactive/cyber-operations (accessed 20 October 2018)

DHS, U.S. (2018). U.S. Department of Homeland Security Cybersecurity Strategy. May. Available from: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf (accessed 20 December 2018)

DoD, U.S. (2011). Department of defense strategy for operating in cyberspace. July. Available from: https://www.hsdl.org/?view&did=489296 (accessed 28 January 2019).

DoD, U.S. (2011). Department of defense strategy for operating in cyberspace. April. Available from: http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf (accessed 28 January 2019)

Jang-Jaccard, J. and Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), pp.973-993

Karabacak, B. and Tatar, Ü. (2014). Strategies to Counter Cyberattacks: Cyberthreats and Critical Infrastructure Protection. Critical Infrastructure Protection, 116, p.63.

Newmeyer, K.P. (2012). Who Should Lead US Cybersecurity Efforts?. National Defense University, Fort McNair, DC.

Obama, B. (2010). National security strategy of the United States (2010). Diane Publishing.

Obama, B. (2015). National Security Strategy. Washington, DC.

O'Rourke, R. (2016). A Shift in the International Security Environment: Potential Implications for Defense-Issues for Congress. Congressional Research Service Washington, DC.

Tatar, Ü., Çalik, O., Çelik, M. and Karabacak, B. (2014). A Comparative Analysis of the National Cyber Security Strategies of Leading Nations. In International Conference on Cyber Warfare and Security (p. 211). Academic Conferences International Limited.

Tatar, U., Georgescu, A. and Geers, K. (2017). Strategic Approach to a Fierce Domain: Findings from the Advanced Research Workshop. Strategic Cyber Defense: A Multidisciplinary Perspective, 48, p.1.

Tatar, U., Karabacak, B. and Gheorghe, A. (2016). An Assessment Model to Improve National Cyber Security Governance. In 11th International Conference on Cyber Warfare and Security: ICCWS2016 (p. 312). Academic Conferences and publishing limited.

Trump, D.J. (2017). National security strategy of the United States of America. Washington, DC.

United States White House Office and Obama, B. (2011). International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Washington, DC

United States White House Office and Trump, D.J. (2018). National Cyber Strategy of the United States of America, Washington, DC:

United States Department of Defense (2018). 21st Century Security Environment, Available from: https://media.defense.gov/2018/Feb/02/2001872883/-1/-1/1/21ST-CENTURY-SECURITY-ENVIRONMENT.PDF (accessed 23 October 2018)

Lieutenant Kenneth James is a Cyberspace Operations Officer in the United States Air Force. He is currently a graduate student at the Air Force Institute of Technology studying Cyber Operations. He received his Bachelor's degree in Mathematics from the University of Texas at Austin in 2017.

Dr Anna-Marie Jansen van Vuuren is a research fellow at the University of Johannesburg's Department of Journalism, Film and Television, under mentorship of distinguished Professor Keyan Tomaselli. Her current research includes themes such as history of South African cinema and the role of representation, identity and ideology within media and film texts. Her research has been published in Taylor and Francis and Intellect journals, as well as being presented at various international conferences. She holds degrees from the University of Pretoria (PhD) and Stellenbosch University (MPhil) in South Africa. Apart from lecturing at various tertiary institutions, she has served as a freelance radio producer for the SABC's Current Affairs programmes since 2008.

Prof Joey Jansen van Vuuren (PhD) heading the Computer Science Department at Tshwane University of Technology. She was the coordinator of the Cybersecurity Centre of Innovation for the Council for Scientific and Industrial Research (South Africa) with the centre focusing on the promotion of research collaboration, cybersecurity education and the exchange of cyber threats. As the Research Group Leader for Cyber Defence (CSIR) for 9 years, she gave the strategic research direction for the research group that was mainly involved in research for the South African National Defence Force and Government sectors on Cyber Defence. Her research publications include journal papers, conference papers and book chapters on cybersecurity governance. She has presented on several forums including national and international conferences and has also been invited as keynote speaker at international conferences.

Dr. Saltuk Karahan is a Lecturer in Old Dominion University's Department of Political Science and Geography. He is also the Program Coordinator for ODU's Center for Cybersecurity Education & Research. Prior to this position, Dr. Karahan worked in Virginia Modeling, Analysis and Simulation Center and NATO Allied Command Transformation.

Martti Kari is university teacher and PhD student in Jyväskylä University. He has MA in Cyber Security (2017) and MA in Russian language and literature (1993) in Jyväskylä University. The subject of his PhD study is Russia´s Cyber Threat Perception and Response to this Threat. He retired in the end of 2017 from Finnish Military Intelligence. His rank is Colonel and his last post before retirement was Assistant Chief of Defense Intelligence.

Dr Shadrack Katuu is an information management specialist. He has worked in various institutions including the University of Botswana, the Nelson Mandela Foundation, the International Monetary Fund, the United Nations peacekeeping and the International Atomic Energy Agency. He is a Research Fellow at the University of South Africa and has authored several publications (see http://goo.gl/sJ3qBG).

Douglas Kelly, Ph.D., MBA, has extensive experience across multiple research, entrepreneurial, consulting, defense, and academic organizations. His current positions include Adjunct Associate Professor at University of Maryland University College; Assistant Professor of Cybersecurity, Math & Computer Science at Webster University; and Senior Professional Staff at Johns Hopkins University/Applied Physics Laboratory.

Faith Lekota is a Senior Manager IT Planning and Governance at the Air Traffic and Navigation Services (ATNS). She is a PhD Computer Science candidate the the University of Johannsesburg and holds a Masters Degree in IT. Her research interests include information security, aviation cyber security, cyber security frameworks, and information security best practise standards.

Christoph Lipps graduated in Electrical and Computer Engineering at the University of Kaiserslautern. Born in Pirmasens, Germany in 1986, he started working as a Researcher and Ph.D. candidate at the German Research Center for Artificial Intelligence (DFKI) in Kaiserslautern. His research focuses on Physical Layer Security (PhySec), Physically Unclonable Functions (PUFs) and entity authentication.

Simon Mahlangu currently holds the position of Principal: Business Improvement at Anglo American plc. He has over twenty years' experience in a variety of roles, across the company, and his current role is at the Iron