UNITED STATES NATIONAL SECURITY STRATEGY: A PROBLEM AND A SOLUTION

Name

Course Code: Course Title

Month Date, Year

Introduction

The fundamental tenets of an effective national security strategy include "clear and realistic objectives, coordinated use of the various instruments of national power, appropriately equipped and trained military forces, well-orchestrated military campaigns and effective battlefield tactics"[1]. Moreover, the basic military functions involve the effective development, deployment and orchestration of military forces. These basic aspects of national security have remained the same over history, and they will remain the same for years to come[2]. However, a lot has changed that has seen changes in the elements that constitute these requirements. For example, what constitutes 'realistic' objectives has changed, the use of military force has changed (especially with the rise of terrorism, which utilizes a rather unconventional type of warfare), among others. Case in point, Leonard and Katz[3] write a comprehensive article on the need for a national border security strategy. In their discussion, the two cite the likeliness of the ISIS penetrating the US's "porous southern border"[4]. They also cite several references on illegal immigration and the risks that they pose to US's national security. However, these two focus more on physical borders. Yet, the rise of cyberspace means that the term 'border' is no longer a clearly definite character. Reinsalu notes: "one of the hallmarks of the modern security

[1]Dennis Drew & Donald Snow. Making the Twenty-First-Century Strategy: an Introduction to Modern National Security Processes and Problems (Air University Press: Alabama, 2006), xi

[2] Drew & Snow, xi

[3] Tom Leonard & Joshua Katz. Its Time for a National Border Security Strategy. *War on the Rocks,* September 17, 2014, http://warontherocks.com/2014/09/its-time-for-a-national-border-security-strategy/

[4] Leonard & Katz, 1

environment is that it encompasses much more than traditional 'hard' security and defense, which put emphasis on military strength and resilience"[5].

The cyberspace has become a defining aspect of modern life. By its very nature, the fact that it links nearly- if not entirely- everybody to a central point, cyberspace exposes all the linked to risks of unauthorized invasion[6]. Examples include the US's disruption of Iran's nuclear plans[7] and North Korea's attack on Sony[8]. Previously, the US's security departments have also been attacked.

Indeed, the biggest threats facing US's national security plays out in the cyberspace. In fact, current reports show that cyber-attacks are becoming an even bigger problem than terrorism[9]. Although terrorists may still utilize the cyber-attacks, another major terror attack on US's soil (like the 9/11) is more unlikely. In other words, cyber-attacks are becoming an increasingly major threat to US's national security than terror.

In a nutshell, with the digitization of all US documentation, the likely exposure of US's security plans makes it possible for unauthorized persons (both within and without the US) to

---

[5] Urmas Reinsalu. The "Internet of Things" Holds Golden Promises, but also Daunting Cyber-Threats" (Security & Defense Agenda Report: Geert Cami, 2013), 27

[6]Reinsalu, 28

[7]David Sanger. Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times,* June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0

[8]Ken Lovett. Former Gov. George Pataki: U.S. Should Declare 'Cyber War' on North Korea. *New YorkDaily News,* December 21, 2014, http://www.nydailynews.com/blogs/dailypolitics/george-pataki-u-s-declare-cyberwar-north-korea-blog-entry-1.2052478

[9] Luis Martinez. Intel Heads Now Fear Cyber Attacks More Than Terror. *ABC News* March 13, 2013, http://abcnews.go.com/Blotter/intel-heads-now-fear-cyber-attack-terror/story?id=18719593

counter these strategies. In other words, cybersecurity becomes a central factor in US's national security strategies.

This paper is a review of the role of cyberspace in US's national security strategies, focusing on the problems, and suggesting solutions.

The Cyberspace and US's National Security Strategies: Problems and Solutions

With skill and perseverance, foreign opponents have been able to penetrate US computer networks (which are poorly-protected) and collect valuable and sensitive information. So far, USs most sensitive military communications have remains safe. However, economic competitors, as well as potential military opponents (such as North Korea) still have relatively easy access to intellectual property of US's leading companies, military technology and government data[10].

Cyber-attack is a relatively novel threat to US's national security, as well as that of its allies. The immediate risk has to do with the economy[11].

The business plans of most US companies involve using cyberspace to interact with their customers, deliver services, and manage supplychains. Moreover, intellectual property is now stored in digital forms. This is increasingly true in this age of cloud technology. Drew[12] notes that more and more information is getting stored in what he calls 'cloud storage networks'. Confirming this observation, a survey by Elastica showed that cloud storage is today very high,

[10] Center for Strategic and International Studies (CSIS). *Securing Cyberspace for the 44th Presidency: a Report of the CSIS Commission on Cybersecurity for the 44th President.* (Washington, DC, 2008), 11

[11] CSIS, 11

[12] Shawn Drew. Android Security and BYOD: Moving in the Right Direction. *Midsize Insider,* August27, 2014, http://midsizeinsider.com/en-us/article/android-security-and-byod-moving-in-the#.VGR5qrF9laQ

and that every employee today storesabout 2,000 documents (on average) in the clouds. Moreover, these employees also 'broadly share' with others about 185 documents (also on average) through the cloud. But there are many risks associated with cloud technology. The Elastica survey showed that 20 percent of the documents that employees 'broadly share' contain sensitive information. Yet, it is worth noting that 13 percent of these stored and 'broadly shared' documents had no controls or limitations against breach.Unfortunately, "weak cybersecurity dilutes our investment in innovation while subsidizing the research and development efforts of foreign competitors"[13].Indeed, in the new global competition, economic strength and technological leadership are as key to national security as military force. Failures of the US to secure its cyberspace puts it at a disadvantage.

For about three decades, the US has struggled unsuccessfully to find counter a response to the threats in the 'new' world. One of the biggest reasons why the US has faced this challenge has to do with the fact that the direction and pace of change in the international environment far-exceeded expectations as well as the ability of the US to predict new change directions. In other words, for a long time the US could not easily discern the potential threats they would face, what would be the key tools of influence and which new opponents would arise. As a result, for a long time the US found itself in a sort-of trance, a strategic indecision that put it at risk[14].

Thankfully, these elements have become increasingly discernible over the last decade. This environment is highly competitive. However, this competition does not take the traditional superpower-confrontation form. Cooperation and completion, as well as conflict, to a certain level, have become routine elements in the new international environments, which has also

[13]CSIS, 11
[14] Ibid, 12

influenced the US's interactions with other nations. Also, in this 'new' environments, particularly in the cyberspace, fleets, armies and military alliances have become- and are increasingly becoming- irrelevant, or at least less important in nations' pursuit or technological progress and economic growth, creation of new ideas and products, and the protection of their informational advantages. Gaining an upper hand in these respects is more important than the accumulation of conventional forces[15].

The US's national security strategy, even years into the new millennium and after the 9/11 attacks, remains largely shaped by the past, and wedded to old threats alliances and strategies. For example, in designing a cybersecurity framework in 1998, a presidential commission under-interpreted the problem. The commission expected that the cyber-attack related damages would be physical (such as the crashing of airplanes and opening of floodgates) and ignored the informational aspect, which has ultimately become the central problem[16].

Coming to power, one of the top national security priorities for the Obama administration was to enact a cybersecurity bill. However, in 2012, the bill was blocked by a Republican filibuster. This divided the house further, with many proponents arguing that the move had stalled a key national security matter and for which the country was least prepared. But it is worth noting that the bill still seemed to take a more physical-impacts approach. For instance, according to Scmidt, the bill was supposed to establish "optional standards for the computer standards that run the country's critical infrastructure, like power grids, dams and

[15] Ibid, 12
[16] Ibid, 12

transportation"[17].The US has, for a long time, relied on what CSIS refers to as "industrial-age government and industrial-age defense"[18].

Despite the politics at the national level, various departments and organizations have taken their own initiatives to curb the problem of cybersecurity- although even these moves were in accordance with National Security Strategy. The Department of Defense (DoD), in collaboration with its interagency and international partners drew its own cybersecurity framework with the aim of mitigating the potential risks that the country and its allies faced, as well as focusing on respecting and protecting the privacy, civil liberty and free expression principles[19]. In this respect, the DoD framework aimed to promote five key strategic initiatives. First,treating the cyberspace as an operational platform for organizing, training, and equipping the DoD. In this respect, the DoD aimed to focus on organizing the cyberspace into a manageable domain that DoD can use to its advantage towards strengthening national security. By the direction of the National Security Strategy, the DoD sought to increase the synchronization and coordination of service components inside each military branch[20].

Second, the employment of new concepts of defense operating to protect the networks and systems of the DoD. This initiative would focus more on implementing constantly evolving operating defense concepts. This was to involve the DoD's enhancement of the best practices of

[17]Michael Schmidt. Cybersecurity Bill is Blocked in Senate by G.O.P. Filibuster. *The New York Times,* Aug. 02, 2012, http://www.nytimes.com/2012/08/03/us/politics/cybersecurity-bill-blocked-by-gop-filibuster.html

[18]CSIS, 12

[19]Department of Defense (DoD). Strategy for Operating in Cyberspace, July 2011, 2

[20]DoD, 5

cyber hygiene; deterrence and mitigation of insider threats; computing architectures, among others[21].

Third, partnering with other US governmentagencies and departments, as well as the private sectors to strengthen collective security. This was aimed to enable as whole-of-government approach[22].

Fourth (which is an expansion of the partnering aspect), building of robust relationships with other allies of the US on the international stage to also strengthen collective security. Like the initiative above, this was also aimed at improving a collective approach to dealing with cybersecurity[23].

Without doubt, this is a very critical ingredient in cybersecurity. Besides, cyberspace spans the entire globe, and because of such as wide scope, no single nation can successfully secure it alone. Moreover, strategies focusing more on domestic goals and actions will always prove inadequate in addressing this problem. The US has for a long time not recognized or given enough attention to the international aspect of cybersecurity. Therefore, by bringing in the international aspect to this issue is very important.

However, this international involvement is easier said than done. In other words, the question is how to involve the international partners.In the past, the US has used its big-brother power over its allies and partners. Over the last decade, China's presence in Africa has grown as the popularityand influence of the US in the continent dwindles- what has come to be referred to

[21]Ibid, 6
[22]Ibid, 8
[23]Ibid, 9

as Africa 'looking East'[24]. To explain this trend, many have cited what is seen as the differences in approach between what has for long been termed as the 'Washington Consensus' (that is, the US's way of doing things in relation to its foreign policy) and the relatively novel 'Beijing Consensus' (that is, China's behavior in its foreign policy pursuits)[25]. The Washington Consensus has largely been seen as heavy-handed, using its power and force to impose on the weaker players (countries)[26]. The largely failed Structural Adjustment Plans, which was forced on many developing countries, is a case in point[27]. Far from this heavy-handedness, the Beijing Consensus has been seen as respectful; that China approaches the developing countries as a partner and on the basis mutual-respect and benefit[28]. Of course, it is doubtful that Africa is benefiting equally as China is. In fact, it may be that this relationship is in reality too one-sided and China is reaping benefits at the expense of the African countries[29]. But this is debatable. However, what remains clear is that Beijing Consensus seems to be doing what the Washington Protocol has failed at for many years, drawing allies closer- not pushing them away[30]. Against this backdrop, therefore, the US must look to win over allies, rather than taking a superiority stance at the expense of mutualrespect.

In this respect, this strategy calls for a coordinated international plan that focuses on norms; that is, behavior expectations and models. But this should be based on fairness. In other

---

[24] Deborah Brautigam. *The Dragon's Gift: the Real Story of China in Africa,* (Oxford: Oxford University Press, 2009), 13

[25]Stephan Halper. *The Beijing Consensus: How China's Authoritarian Model Will Dominate the Twenty-First Century,*(New York: Basic Books, 2010), 26

[26] Harper, 26

[27] Ibid, 27

[28] Vivien Foster, William Butterfield, Chuan Chen &Natalyia Pushak.*Building Bridges: China's Growing Role as Infrastructure Financier for Sub-Saharan Africa*, (Washington: The World Bank, PPIAF, 2009)

[29]Brautigam, 9

[30] Foster, et al., 18

words, the US must recognize the internal political contexts of these countries and in what ways they differ from them. CSIS[31] proposes the use of sanctions against countries that harbor cyber criminals- to reinforce the so-called international norms. However, the use of sanctions is the same high-handedness that has sidelined the US over the US, and which (as already noted above) has provided a hole that China has gladly exploited. Besides, while it is true some countries may not readily cooperate with the US in this respect, sanctions have also proved largely ineffective[32]. Therefore, the US should recognize the internal legal constraints that may make it hard for countries to take action against cyber criminals. Accordingly, CSIS notes: "no nation can be an effective partner in fighting international cybercrime unless it has in place both the domestic laws and operational expertise to do so"[33].Moreover, by its very nature, cybercrimes can be hard to detect, and many countries may lack the means to identify the criminals. The US may be one of the key targets of cybercrime. But it is also probably one of the countries that harbor the highest number of cybercriminals- at least in numbers if not in percentages. Simply, this strategy should be based on mutual-respect, and sanctions should not apply. Instead, the US could help these countries establish the right legal framework to fight cybercrime. The problem is that the US itself is also struggling with such a legal framework. As the saying goes, *Charity begins at home,* and the US should lead by example.

[31]CSIS, 21

[32] Julia Grauvogel & Christian von Soest. *Claims to Legitimacy Matter: Why Sanctions Fail to Instigate Democratization in Authoritarian Regimes*. German Institute of Global and Area Studies (GIGA), Working Paper No.235, 2013), 5

[33] CSIS, 21

Finally, leveraging of the country's ingenuity through a strategic cyber workforce and fast technological innovation. This was to focus more on the cyber workforce, with the aim of utilizing the country's talent and expertise towards dealing with this problem[34].

Indeed, information security is not just about technology, but also about the knowledge and skills, awareness and intentions of employees as well as customers (and other stakeholders) who use the information-based systems and networks[35]. In this respect, the development of IT takes into consideration not just the needs, but also the people who will use them. However, humans are more prone to mistakes and misunderstandings; are more susceptible to various motivations, good and bad; and can be affected by stress (internal and external). All of this can potentially affect the actions of the humans who use these IT tools. Above this IT is changing human behavior (individual and social) in many ways, which are likely to have serious impacts on information security. Social networking sites, for example, can help users develop trust and establish communities based on shared interests. But criminals and terrorists can manipulate such groups (on the basis of fake trust) for the wrong reasons. Besides, users in support sites are more likely to open up and expose many private details.

Generally, according to Wybourne et al.[36], security interventions based purely on training programs have not been inadequate in dealing with the problem of cybersecurity. Sometimes employees cannot comply with security policies and processes even when they want to. Cognitive psychologists find that even well-intentioned users often forget, ignore or misinterpret

[34]DoD, 10

[35] Martin Wybourne, Martha Austin & Palmer Charles. *National Cyber Security: Research and Development Challenges Related to Economics, Physical Infrastructure and Human Behavior,* (Institute for Information Infrastructure Protection: an Industry, Academic and Government Perspective), 23

[36]Wybourne et al., 27

important information. This may have to do with the fact (based on evidence) that humans tend to focus more on what they believe is important. But in the process, an individual may ignore what they think is irrelevant, and end up missing important things that should influence their response. There are also the influences of social norms at the workplace.

The Senate has since made a big move towards expanding the scope of these initiatives. For example, despite president Obama threatening a veto after the failed effort in 2012, in the end the House passed a bill that would encourage intelligence agencies to share information with the private sector (businesses) regarding threats on computer systems, including the attacks by Chinese hackers on American Websites[37]. Indeed, this move to involve the private sector is an important one. Besides, the private sector runs a huge chunk of the country's infrastructures. For instance, Department of Homeland Security[38]statistics show that the private sector owns and manages an estimated 85 percent of the country's critical infrastructure. Corporations, for example, critically depend on IT systems on majority of the business processes, as well as the tracking of their corporate data. In other words, by involving the private sector, the government increases its tracking abilities. Therefore, the government is in a better position to deal with the problem.

In all these discussions, these initiatives seem to focus more on external threats. The ongoing conflict between the US and North Korea on cyberspace is a good example.The debate is divided over whether it is already a cyberwar or not with the George Pataki (a former US

[37] Robert Pear. House Votes to Approve Disputed Hacking Bill. *The New York Times,* April 26, 2012, http://www.nytimes.com/2012/04/27/us/politics/house-defies-veto-threat-on-hacking-bill.html

[38] Department of Homeland Security, in Wybourne, Austin &Charles, 7

Governor) asserting that the US should declare a 'cyber war' on North Korea[39]. The debate aside, though, the situation has still raised alarm in the US, and therefore demonstrates how external forces plays a key role on cyberspace and national security.

However, even though external forces remain real, there is a genera shift that in which internal threat is increasingly becoming bigger. This has to do with hitherto too much focus on counterterrorism. In fact, counterterrorism has been the main theme when discussing national security for more than the last decade. This tendency implies a general assumption that counterterrorism policies are in and of themselves national security policy and/or strategy. However, counterterrorism is only a small matter in the broader discussion of national security. In other words, cybersecurity must fit within the wider context of national security strategy[40].

Conclusion

This essay has reviewed United State's cyber-security efforts, with the aim of citing problems, and finding solutions. Indeed, as this essay shows, the US has increasingly paid attention to cybersecurity. Collaboration with other partners (locally and internationally), for example, is a clever move that utilizes human capital and other resources towards this endeavor.However, the government has not been able to launch a successful answer to the risks in cyberspace. This may be attributable to politics, but also- most importantly to the lack of understanding of the real nature and scope of this threat. For example, there seems to be too much focus on the physical impacts of cybercrime. In the process, the informational aspect has largely been ignored. This is an under-definition of the problem.

[39] Lovett, 1
[40] Colucci, 1

To provide a real answer to the problem starts with acknowledging that the informational aspect is the biggest problem (and everything else, including physical impacts, only stem from it). Secondly, the initiatives toward cybersecurity have focused more on counterterrorism than on national security. Counterterrorism, as Colucci[41] argues, is only a small part of national security. This is another case of under-definition and/or under-conceptualization. Besides, while cyber-attacks happen every day, it is highly unlikely that another major terror attack like the 9/11 attacks will happen again.This emphasis on counter-terrorism means the government focus more on external forces than internal forces (such as fun 'hacktivists'), which may be a big help to to other security risk factors.

Unlike in the past decade, the US should not be caught by surprise, but be able to anticipate future changes.In other words, the first step toward an effective cybersecurity rests on a proper understanding of the problem, its nature, scope and evolution. Besides the matter of definition and conceptualization, there are also certain general challenges that US's cybersecurity interventions are likely to face as a consequence of the nature of the internet, such as infrastructural and human-factor problems, which may not be easy to deal with because they do not have easy answers.

[41] Ibid, 1

Bibliography

Brautigam, Deborah. *The Dragon's Gift: the Real Story of China in Africa.* Oxford: Oxford University Press, 2009, 13

Center for Strategic and International Studies (CSIS). *Securing Cyberspace for the 44th Presidency: a Report of the CSIS Commission on Cybersecurity for the 44th President*, (Washington, DC, 2008), 11

Colucci, Lamonti. U.S. National Security Strategy Must Go Beyond Counterterrorism. *U.S. News*, Jan. 17, 2013. http://www.usnews.com/opinion/blogs/world-report/2013/01/17/us-national-security-strategy-must-go-beyond-counterterrorism

Drew, Dennis & Donald Snow. *Making the Twenty-First-Century Strategy: an Introduction to Modern National Security Processes and Problems*, (Air University Press: Alabama, 2006), xi

Drew, Shawn. Android Security and BYOD: Moving in the Right Direction. *Midsize Insider,* Aug. 27. 2014. Retrieved 17 November 2014, http://midsizeinsider.com/en-us/article/android-security-and-byod-moving-in-the#.VGR5qrF9laQ

Foster, Vivien, William Butterfield, Chuan Chen & Natalyia Pushak. *Building Bridges: China's Growing Role as Infrastructure Financier for Sub-Saharan Africa*, (Washington: The World Bank, PPIAF, 2009)

Grauvogel, Julia & Christian von Soest. *Claims to Legitimacy Matter: Why Sanctions Fail to Instigate Democratization in Authoritarian Regimes.* German Institute of Global and Area Studies (GIGA), Working Paper No.235, 5

Halper, Stephan. *The Beijing Consensus: How China's Authoritarian Model Will Dominate the Twenty-First Century*. New York: Basic Books, 2010, 26-27

Leonard, Tom & Joshua Katz. It's Time for a National Border Security Strategy. *War on the Rocks,* Sept. 17, 2014. http://warontherocks.com/2014/09/its-time-for-a-national-border-security-strategy/

Lovett, Ken. Former Gov. George Pataki: U.S. Should Declare 'Cyber War' on North Korea. *New York Daily News,* December 21, 2014, http://www.nydailynews.com/blogs/dailypolitics/george-pataki-u-s-declare-cyberwar-north-korea-blog-entry-1.2052478

Martinez, Luis. Intel Heads Now Fear Cyber Attacks More Than Terror. *ABC News* March 13, 2013. http://abcnews.go.com/Blotter/intel-heads-now-fear-cyber-attack-terror/story?id=18719593

Pear, Robert. House Votes to Approve Disputed Hacking Bill. *The New York Times,* April 26, 2012. http://www.nytimes.com/2012/04/27/us/politics/house-defies-veto-threat-on-hacking-bill.html

Reinsalu, Urmas. *The "Internet of Things" Holds Golden Promises, but also Daunting Cyber-Threats"*, (Security & Defense Agenda Report: Geert Cami, 2013), 27

Sanger, David. Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times,* June 1, 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0

Schmidt, Michael. Cybersecurity Bill is Blocked in Senate by G.O.P. Filibuster. *The New York Times,* Aug. 02, 2012, http://www.nytimes.com/2012/08/03/us/politics/cybersecurity-bill-blocked-by-gop-filibuster.html

Wybourne, Martin, Martha Austin & Palmer Charles. *National Cyber Security: Research*

and Development Challenges Related to Economics, Physical Infrastructure and Human Behavior. Institute for Information Infrastructure Protection: an Industry, Academic and Government Perspective, 7