SECURITY TECHNOLOGY POLICY PAPERS SERIES 1

Spring | 10

Obama's Cybersecurity Plan

Marianne STONE
Geest-MSH - Paris
Sciences Po – Paris
Columbia University, School of International and Public Affairs – New York

"THE NATION IS AT A CROSSROADS"[1]

The digital age is here. With new technologies emerging everyday, the world has become heavily dependent on the way of the future. However, with the good, so come the challenges. Cyberattacks and cybercrimes are on the rise, the most recent being in 2009 aimed at American and South Korean government websites as well as other important organizations and the 2008 attack on the Pentagon. These are only a few examples of an issue that has produced a significant amount of concern in the past several years.

The EU has already created its cyber security agency under the name of ENISA – The European Network and Information Security Agency[2]. Presented as the "pacemaker" for Information Security in Europe, its mission is to help the EU Commission, the member states and the business community to address, respond and especially to prevent network and information security problems. Compared to European responsiveness and reactivity against such issues, the US has often appeared as being behind the wave. Even if Internet security has been a crucial issue in the US, it took time for authorities to take federal measures to fight against cyber attacks.

By addressing cybersecurity as critical to the US national security, public safety and personal privacy and civil liberties, president Obama decided to transform it into a vital issue both for the nation and citizens. In 2009, the Obama administration, therefore, set out to formulate a strategy for cybersecurity in order to address the threats that the President likens to "weapons of mass *disruption*"[3].

Before Obama's, the Bush administration had launched the government's Comprehensive National Cybersecurity Initiative (CNCI) in 2008 under a shroud of secrecy generating sharp criticisms from privacy and civil liberties groups. The initiative had 12 directives covering military, civilian, government networks and critical infrastructure systems, but for critics it was unable to provide sufficient guarantees that the pursuit of cybersecurity will not include monitoring private sector networks and the Internet traffic.

The Cyberspace Policy Review, a 40 page "clean-slate" review initiated by president Obama to "assess US policies and structures for cybersecurity", offers a strategic look into what the government considers to be a major issue. The review represents the first step of the President's pledge to "lead an effort, working with private industry, the research community and our citizens, to build a trustworthy and accountable cyber infrastructure that is resilient, protects America's competitive advantage, and advances our national and homeland security."[4]

For the purpose of the review cyberspace is defined as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controller in critical

---

[1] The White House, *Cybersecurity Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. April 2009, iii.
[2] http://www.enisa.europa.eu
[3] Markoff, J and Sanger, D., "Obama Outlines Coordinated Cybersecurity Plan*", The New York Times*, May 30, 2009.
[4] The White House, *Cybersecurity Policy Review*, B-1.

industries. Common usage of the term also refers to the virtual environment of information and interactions between people".[5]

The review recognizes that the federal government is not yet equipped to deal with a full-scale cyber assault in an effective way. The risks that cyber attacks pose present the United States, as well as the international community, with challenges that will likely prove difficult to maneuver. Dependence on technology has provided opportunistic enemies with a new method of warfare, one that is difficult to trace, nearly impossible to prosecute, and even harder to legally define.

MAIN GOALS

The policy review focuses on a number of issues that affect or are affected by cybersecurity. Ranging from short to mid-term plans, the document attempts to reorganize the complex approach of the past. Despite the strides gained in the past two years by the previous administration with its Comprehensive National Cybersecurity Initiative (CNCI), much improvement is still needed. This is a recurring theme in the policy review, which organizes its main goals as follows:

- ***Lead from the Top***: Ultimately, the White House is responsible for taking the initiative to update the nation's capability to deal with cyber threats, as well as other related issues such as legal norms.

- ***Building capacity for a Digital Nation*****:** While cybersecurity has been on the government's radar for some time, the general public has little awareness on the issue. Increasing this awareness will help everyday Americans to make smarter choices and manage risks in a more efficient way.

- ***Sharing Responsibility for Cybersecurity***: The issue of cybersecurity is global. Public as well as private sectors, national as well as international actors must all be involved in the process for it to succeed. Collaboration between sectors as well as on an international level should be explored,

- ***Creating Effective Information Sharing and Incident Response*****:** The response effort should be centralized around a cybersecurity official appointed by the president. The framework for response should be clear and unified with enhanced information sharing to improve capabilities.

- ***Encouraging Innovation*****:** Fostering development of new and improved technologies through innovative research and development that could contribute to a more secure cyberspace. This should be coupled with new authenticating technology (i.e. identity management and biometrics) to ensure data exchange is trustworthy.

Based on these goals, the plan offers both near-term and mid-term action plans some of which, for example appointing a "cyber czar", have already been implemented. Other important aspects of these plans, however, will be more difficult to execute. For example, the near-term plans of interagency cleared legal analyses and the organization

[5] The White House, *Cybersecurity Policy Review, op.cit, p1.*

of a nation-wide education campaign to raise awareness of cyber threats. The former seems to be an endemic problem for many security related issues: the lack of interagency cooperation and coordination creating gaps and deficiencies across the board. The latter will take manpower, funds and time and seems likely to take the back seat to other issues deemed more pressing.

The mid-term action plan is subject to similar criticism. The perennial problem of resolving interagency disputes appears as the highest priority for mid-term action. Both this and the goal of expanding information sharing with key allies to seek bilateral and multilateral arrangements to improve interest, all the while protecting civil liberties and privacy rights, are daunting tasks. However, the tasks of determining mechanisms for incident response and developing scenarios and metrics that can be used for risk management seem to be more easily attainable.

In order to avoid criticisms of secrecy, president Obama decided to declassify part of the plan in March 2010[6]. But this portion includes information on only part of the initiative and does not discuss cyberwarfare as a strategic goal[7]. Instead, it focuses on the deployment of Einstein 2 and Einstein 3, intrusion detection systems on federal networks designed to impact internet traffic entering government networks to detect potential threats like malicious content. But these programs have already raised concerns because they involve scanning the content of communications to intercept malicious code before it reaches government networks.

A COMPREHENSIVE, ORGANIZED STRATEGY?

What is clear from the administration's move towards an updated strategy is that the existing state of affairs is no longer considered adequate. Agencies, for example the Department of Homeland Security and the National Security Council need to be organized to be able to not only prevent, but also respond quickly to any further cyber attack in order to protect national security. In fact, "The Administration already has established an Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC), chaired by the National Security Council (NSC) and Homeland Security Council (HSC), as the primary policy coordination body for issues related to achieving an assured, reliable, secure, and survivable global information and communications infrastructure and related capabilities."[8] However, the goal to defend the national territory and protect its citizens becomes more difficult in the intangible realm of cyberspace. The review recommends a "shared responsibility" between the public and private sectors for these tasks, recognizing that alone, little will be possible.

The current situation of overlapping authorities distributed over a wide array of federal departments, none of whom carry enough decision authority, needs to be updated. However, while this seemingly paramount issue is pointed to in the preface of the review, the solution offered is vague. An "integrated approach" of the different federal agencies involved is seen as optimal. However, one wonders if reconciling agencies such as the National Security Agency (NSA), the Homeland Security Department and the

[6] "US Declassifies Part of Secret Cybersecurity Plan", March 2, 2010, www://wired.com/threatlevel/2010/03us-declassifies-pa
[7] *Ibid.*
[8] The White House, *Cybersecurity Policy Review*, op.cit, p.7.

Pentagon who have been engaging in "turf wars" over this very issue is even possible. If it is not, can the strategy ever claim itself to be "comprehensive and organized"?

And the federal government is only the beginning. The review addresses on several occasions the need for a public-private partnership, acknowledging that the private sector is the leader when it comes to innovation and that it "designs, builds, owns, and operates most of the network infrastructures that support government and private users alike". It is, therefore, desirable that a public-private partnership have a clearly defined goal with clear-cut roles and divisions of responsibilities and that obstacles to achieving an optimal partnership be identified.

The key solution that is offered to address the issue of integrating the oftentimes-overlapping responsibilities of the many different agencies is the appointment of a "cybersecurity policy official", more commonly known as the *cyberczar*. The appointment of the cyberczar who reports to the National Security Council (NSC) was made official on December 22, 2009 with the appointment of Howard Schmidt to the position.

Howard Schmidt comes to the position with extensive experience in business, law enforcement and government. He formerly held the position of chief security officer at Microsoft as well as vice president and chief information security officer at E-Bay; currently his is president of the Information Security Forum, a non-profit "working to resolve cybercrime and cybersecurity issues"[9]. Additionally, he served as special advisor for cyberspace security under the Bush administration from 2001-2003 being a driving force of the largely-ignored "National Strategy to Secure Cyberspace".

While the appointment of Howard Schmidt was not a surprise, the lengthiness of the process was somewhat unexpected. However, many believe that there is wide speculation and concern that the position will entail a large responsibility with "little true authority"[10] However, based on the cyber review document, the position would be *the* coordinator over all the different federal agencies involved, and while it seems that there would be some real difficulties involved in maneuvering through the different competing agencies, the President has reassured that the new coordinator will be an "action officer", one who would have "regular access to me"[11].

This being said, many critics are skeptical as to whether one person would be able to successfully delegate tasks to the different agencies in a way that would not ruffle any feathers and, at the same time, not fall into the same pattern of overlapping responsibilities. To say the least, Schmidt has his hands full with a position for which many have very low expectations.

ENGAGING THE NATION AND THE PRESERVATION OF CIVIL LIBERTIES?

In the post 9/11 world, statutes such as the Patriot Act have contributed to a loss of the American people's confidence that the federal government takes the civil liberties and privacy rights seriously. It is, therefore, of the utmost importance that these liberties not

[9] Nakashima, Ellen and Wilgoren, Debbi., "Obama names Howard Schmidt as cybersecurity coordinator", *The Washington Post*, December 22, 2009.
[10] *Ibid.*
[11] Sanger, D and Markoff, J., "Obama Outlines Coordinated Cybersecurity Plan", *The New York Times*, May 30, 2009.

be forgotten, and that there exists some degree of transparency in the new strategy so that the American people can put their trust in this new initiative.

In the number 4 slot of the near-term action plan the designation of a "privacy and civil liberties official to the NSC cybersecurity directorate" seems to be a step in the right direction. In fact, the importance of building and maintaining trust between "civil liberties and privacy community, the public and the program for cybersecurity" is referenced with importance throughout the document. However, it is unclear how this will be addressed beyond the near-term recommendation.

The "communications" portion of the policy review could also contribute to formulating not only a more trustworthy strategy, but one that actively engages the American people to increase awareness about the realities of cybersecurity. This aspect of the review has produced little to no coverage, and yet it indicates that the strategy hopes to involve the American people and increase cybersecurity education in a way that it hadn't with previous administrations.

In this respect, it is important to remember that the nature of cyberspace is one that has the ability to cause harm on multiple levels. While cyber assaults on areas that affect national security are momentous and create media frenzies, one must not forget the potential economic and everyday aspects of cyberspace that could be targeted. From identity theft to hacking into the computerized controls on oilrig settings[12] to hospitals, it seems as though nothing is safe from the vastness of cyberspace. Therefore, the plan to educate the American people on the diverse threats seems to be a step in the right direction, although one that could prove burdensome in terms of cost.

If education seems to be a good step, there is however a need for a real transparency about the focal objects and all directions of cybersecurity which is still considered as an issue of national security. Critics keep on expressing reservations about the "transparency discourse" assuming that all is not correctly addressed. Moreover, since in the context of the fight against terrorism controlling citizen's communications is still favored as a useful action for fighting against terrorism, this raises great concern that needs to be taken into consideration by the administration.

CYBERWARFARE: THE COMPLEX WAVE OF THE FUTURE?

One aspect of cybersecurity that has yet to be addressed by the Obama administration is the role that the military will play in what seems to be the future of warfare; a new era composed of code and cyberweapons that can reach in and attack without a visible trace.

Cyberwar is unlike traditional warfare in many ways. With questions of sovereignty, territorial jurisdiction and the definition of force hard to answer, one might wonder if the military is a good fit for this type of "virtual" combat. For these reasons, questions and concerns dealing with "military effectiveness, legality and morality"[13] have been raised. With unknown consequences and collateral damage almost certain, there is a difference of opinion between those who believe the concern to be "excess caution on

[12] Grant, G., "The New Threat to Oil Supplies: Hackers", *Foreign Policy*, August 25, 2009.
[13] Markoff, J and Shanker, T., "Halted '03 Plan Illustrates U.S. Fear of Cyberwar Risk", *The New York Times*, August 2, 2009.

the part of Pentagon planners"[14] and those who worry about unintended consequences such as "taking out a hospital which is sharing a network with another agency"[15].

It is unclear how the military will fit in to the Obama administration's strategy, but the issue of legal norms linked to this issue "present serious challenges to achieving a safe, secure, and resilient digital environment."[16] Currently, cyberwar poses problems when it comes to the laws of war. With *jus in bello* (laws of war), its customary practices, as well as documents such as the Geneva Conventions and the United Nations Charter having taken form during a time when war was defined in a traditional sense, cyberwar proves difficult to define within this context. As Jack L. Goldsmith, a professor at Harvard Law School observes, force is a central concern. "The UN charter basically says that a nation cannot use force against the territorial integrity or political independence of any other nation. But what kinds of cyberattacks count as force is a hard question, because force is not clearly defined."[17]

Obama's plan recognizes that the legal norms, albeit domestic or international, have not yet caught up with the current state of affairs. The policy review acknowledges this and cites the future cybersecurity policy official as the person who should oversee movement on this issue, bringing law and policy up to speed with one another in order to adequately address this issue.

MOVING TOWARDS THE FUTURE: NO TURNING BACK?

As stated in the executive summary of the policy review: "the status quo is no longer acceptable". Whether or not one agrees with all or part of the suggestions found in the policy review, the fact that previous efforts are falling short is clear.

Reactions to the strategy have been "cautious optimism", with a lot of individuals wondering what the implementation of the strategy will actually look like. What is clear from most security experts is that the choice of the cybersecurity policy official is pivotal Schmidt is clearly well qualified and highly capable. However, some doubt that the position will allow him the authority to really make the headway needed on this issue. The cyberczar is seen as someone who needs to be able to perform on multiple different levels and wear many hats. The responsibility of getting the different federal agencies to work together, tackle the legal and civil liberties issues as well as working on educating the nation, just to name a few, seems like a lifetime of work. When the review came out, many experts seemed to be holding judgment not for the administration's strategy, but for the person who will be filling some large shoes. With the appointment now made, people are now worried that the position, itself, would be difficult for anyone to successfully maneuver. Howard Schmidt's first address as cybersecurity coordinator shows that he has a clear understanding of what is expected of the position. However, it remains to be seen if he will be successful in navigating the bureaucratic waters of Washington. Only time will tell.

BIBLIOGRAPHY:

---

[14] *Ibid.*
[15] *Ibid.*
[16] The White House, *Cybersecurity Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, April 2009, iv.
[17] Markoff, J and Shanker, T., "Halted '03 Plan Illustrates U.S. Fear of Cyberwar Risk", *The New York Times*, August 2, 2009.

Center for Strategic and International Studies. 2008, *Securing Cyberspace for the 44th Presidency.* Washington, DC: CSIS.

Grant, Greg. 2009, "The New Threat to Oil Supplies: Hackers." *Foreign Policy*, 25 August.

Hathaway, Melissa. 2009, "Securing our Digital Future." 29 May.

Markoff, John and Thom Shanker. 2009, "Cyberwar - Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk." *The New York Times,* 02 August.

Nakashima, E., & Wilgoren, D. 2009, "Obama names Howard Schmidt as cybersecurity coordinator", *The Washington Post*, December 22.

Sanger, David E. and John Markoff. 2009, "Obama Outlines Coordinated Cybersecurity Plan." *The New York Times,* 30 May.

The White House. 2009, *White House Cyberspace Policy Review Documents* http://www.whitehouse.gov/cyberreview/documents/

The White House. 2009, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure", http://www.whitehouse.gov/cyberreview/documents/

Relevant Government Institutions:

Department of Homeland Security:
http://www.dhs.gov/index.shtm

National Security Council / The White House:
http://www.whitehouse.gov/administration/eop/nsc/

National Security Agency/Central Security Service:
http://www.nsa.gov/

US Department of Defense:
http://www.defenselink.mil/ and http://www.defense.gov