Rami Khater
Rachel Schaffer

Georgetown University
13 April 2009

## INTRODUCTION

In considering the role of the United States government in addressing cybersecurity both domestically and abroad, we have identified four recommendations we believe can help define the future of cyber-regulation and the international system as represented in the online world. While independent in execution, common themes identified in each recommendation are that of: openness, transparency and collaboration within, as well as across borders. The four recommendations proposed in further detail within this document are:

**1) The introduction of "wiki" technology in cybersecurity planning and social networking**
**2) The creation of public service announcement/all-age educational initiatives to provide citizens the knowledge necessary to do their part in keeping cyberspace secure;**
**3) A comprehensive overhaul of how the international/domestic legal framework distinguishes "crime" in the real world versus that of borderless cyberspace; and**
**4) The creation of an international organization to design and enforce cybersecurity standards across borders, as well as encourage information sharing on the issue between interested nations.**

## I. CYBER-PEDIA

Web 2.0 technologies have been implemented into a number of security initiatives, as demonstrated in the IC's adoption of a Wikipedia-inspired communication technology of "Cyber-pedia." We recommend the creation and adoption of a "Cyber-pedia," dedicated to supporting collective intelligence as it relates to cybersecurity. While we understand the need for a focused initiative such as the 60-day assessment currently being conducted, we hope that the findings lead to a continuous re-assessment of re-emerging threats. It is in part through the creation of Cyber-pedia that we hope the re-assessment will take place.

The state of cybersecurity threats is constantly changing and cannot be viewed as adequate at any point in time. To combat the ever changing threat, the government must setup an internal social network to facilitate communication between cybersecurity experts in all branches of government. Using the Cyber-pedia as the basis for the sharing of knowledge in the social network allows them to be used in tandem as a knowledge repository for government. An added benefit will be the professional relationships that are created and maintained due to the Web 2.0 based technologies. It will encourage camaraderie between individuals in different organizations, thus, by sharing information between branches of government and experts outside those offices, we can build a more unified and secure cyber infrastructure. In times of crisis the network's knowledge repository and relationships can be used to thwart or stem the tide of a cyber attack by making disparate government agencies work together and incorporating insight from experts within the field. As a model of the system, creators could use the Intellipedia framework used within the intelligence community for collective intelligence among analysts.

By adopting technologies that enable the government to be more agile, flexible, open and collective knowledge oriented, the US can better prepare itself to defend against enemies that are similar in nature. The integration of the Cyber-pedia does not completely remove the necessity for traditional methods of collaboration; it instead offers an alternative that will in time become a primary means of collaboration between government workers.

Rami Khater
Rachel Schaffer

Georgetown University
13 April 2009

## II. PUBLIC EDUCATION

Ensuring that the public understands their role in cybersecurity presents a second recommendation requiring direct action by the government to most effectively secure cyberspace. In order for goals set forth by the government to be realized, each individual must recognize the importance of keeping every "node" in the cyber network secure. Due to the quick rise in popularity of the Internet, many users found themselves suddenly reliant upon cyberspace for everything from bill-paying to communication; without any formal introduction to the “do’s” and “don’t” of cyberspace. Without a basic understanding of the functionality of the Internet, the importance of running updates, secure passwords or the danger present in attachments, the public remains a tempting target for those who wish to exploit them. As such, with an ever-growing number of individuals holding email accounts and operating computers from desks at home/work, the likelihood that each person does their part to ensure a fully secure network remains slim. Thus, we suggest the creation of an aggressive public education initiative to address public negligence in technological knowledge, using the already existing National Cybersecurity Awareness Month (NCAM) as a base for such a measure.

While NCAM presents an optimistic start to a public awareness effort, the event could have had a larger impact with more widespread publicity aimed at educating a wider range of citizens. We suggest enhancing and elaborating upon the NCAM message by creating more aggressive and ongoing campaigns targeting various audiences. First, we suggest implementing educational programs within public schools, using DARE as a model for such an endeavor. An organized education campaign targeting school-aged citizens will foster early understanding of cybersecurity efforts as they relate to the individual. Second, we suggest the creation of televised public service announcements and other traditional media to reach older audiences, similar to those surrounding the recent digital TV switch campaign. Finally, we suggest innovative techniques designed to reach more tech-savvy young adults, such as those used the Ydouthink campaign. Together, these measures would present a more open exchange between the government’s stated goals and responsibilities of the individual. Further, they would help arm the public with the education necessary for them to understand and implement the individual elements of cybersecurity as they pertain to the broader problem.

## III. OUTDATED LAWS: DOMESTIC and. INTERNATIONAL FRONTIERS

Laws, both domestic and international, as they currently stand are inadequate when dealing with cyber crimes. We recommend new laws be put in place or current laws be amended to ensure their ability to govern over the changing nature of crime enabled by technology. These laws must consider the impact of the Internet on the ability of crimes to be both domestic and international, with multiple possible jurisdictions. Changes must be made both abroad and at home to ensure criminals may be pursued and brought to justice for cyber crimes they have committed. These sets of international laws must be worked towards diplomatically, in similar ways to international copyright law. On the diplomatic front, nations which refuse to adopt or apply the new laws may have economic sanctions applied and/or be frozen out in other areas of

need, to force compliance.

A fundamental shift in thinking when dealing with cyberspace must be made within the government. Therefore, when laws and policies are viewed, made and amended they must be adaptable and withstand the test of time in the new technology enabled world. The old laws and policies have proven unable to deal with emerging cyber threats. There must be an understanding that the need to move outside of current frameworks and accepted practices will be needed.

## IV. INTERNATIONAL ENTITY[1]

A final recommendation (related to our third recommendation) is the creation of an international entity to address the cross-border nature of cybersecurity. The international stage as a whole may face the negative consequences of one nation's domestic cybersecurity failure due to the interconnectedness of cyberspace. In this way, safeguards and policies adopted in one nation cannot be wholly successful if cyber threats migrate to less-regulated nations to operate. International collaboration bridging domestic initiatives can help ensure each nation's policy compliments those of their allies. In this vein, we suggest the creation of an international body, like the U.N., to collaborate on domestic initiatives and ensure international cooperation in cyber security efforts.

The body would in part be designed to streamline cyber-regulations that affect all nations. In the past, governments worldwide have been reluctant to regulate software and technology companies at domestic or international levels due to the overwhelming belief that it would stifle innovation. This may in part be true, but the financial and real estate sectors provide prime examples of the perils of complete deregulation across and within nations. Currently, software companies are not held liable for software they create that are ultimately proven to be bug-ridden and laden with security holes – problems that not only impact the company's home nation, but all nations where the given software is used. The creation of an international entity could assist governments in holding companies liable in cases of gross negligence on the premise of the international security threat posed by poorly written software. This would be in tune with similar standards and expectations to which many other industries are held accountable.

We recognize, in suggesting such a body, that a shift in the international system regarding what

---

[1] From Sam Visner: This recommendation in particular bears attention. The US Government should encourage and lead development of international cyber-operations rules of conduct consistent with our view of an acceptable approach to international security, and specialized mechanisms to support those rules of conduct. At the same time, the US Government needs to identify those international issues relating to cyber to which US interests are sensitive, build positions pertinent to those issues, and ensure adequate US cyber representation to all international bodies (e.g., the International Telecommunications Union, collective security organizations, and bilateral arrangements) in which these interests are addressed. In doing so, the US Government should ensure that representation is consistent in international bodies and that our positions are reflected consistently across those bodies.

nations are cyber powers compared to the traditional balance of power would be necessary. In creating the entity, while simultaneously keeping the United States interests in mind, we urge creators to understand that a concession of a certain degree of power over the Internet is necessary to maintain a critical level of control in the long-term. Put differently, we again stress the importance of sharing, transparency and collaboration, but this time at the international level. Further, the U.S. can use this opportunity to ensure its continued control of the Internet through soft power by controlling standards committees and other neutral internet bodies. This would preserve a certain power in collaborating with other nations, without a hegemonic threat.

## CONCLUSION

Our recommendations suggest a paradigm shift in government thinking about cybersecurity. We can no longer continue down the same reactionary path, which has begun to show its inability to secure our cyber borders. We strongly suggest a pro-active approach to combating the issue through education, policy, law and international diplomacy. With these initiatives underway, the government must leverage the lessons learned in the private sector and use new technology to help fight the cyberwar as it exists both within and across borders.