21st Century Cybersecurity Challenges, Comments, Solutions, and Path Forward

Dr. Bahador Ghahramani, P.E., CISM, CPE

Abstract. This scientific paper discusses the 21st Century foreseen breakthroughs in the Cloud Computing Technology and how they affect Cybertechnology and our lives.

Cloud Computing technology is moving forward constantly. Therefore, current technology may not be ready and applicable for the future. In addition to updating, the Government should also look to advanced research and development centers for new concepts and innovative principles in the field. In the future, Cloud Computing will be on-line accessed through software applications and shared information with remote server networks. This will eliminate current dependency, primarily, on tools and information located on personal computers. Cloud Computing will also become more dominant than other Internet means of communications. Simply stated, Cloud Computing will be the driving force that permits a user to communicate personal and work related activities securely through connections to servers operated by Cloud Computing sources. Cloud Computing technology is the primary driving force of social networking sites (500 million people use Facebook), webmail services like Hotmail and Yahoo mail, microblogging and blogging services such as Twitter and WordPress, video-sharing sites like YouTube, picture-sharing sites like Flickr, document and applications sites like Google Docs, social-bookmarking sites like Delicious, business sites like eBay, and ranking, rating, and commenting sites such as Yelp and TripAdvisor.

The future of Cloud Computing is bright: it will continue and effectively dominate the Information Technology (IT), Telecommunications Industry (TI), and a host of other information transactions-based technologies because it will allow users to have easy access to individualized, affordable, instantaneous, and accurate cutting-edge information. Cloud Computing will place a personal cloud in each private workstation. Cloud Computing will transform an Internet-based application that runs from smart phones instead of current software running PC. The future of Cloud Computing evolves from development of a more sophisticated desktop-cloud hybrid as a primary method of interface with information.

Background

I was asked by Tom Baer, Deputy Director of National Cybersecurity and Communications Integration Center (NCCIC), to comment on Deputy Under Secretary for Cybersecurity Mark Weatherford's publication, "Cybersecurity Challenges and Solutions on June 5, 2012. In a formal email, Mr. Mark Weatherford states that:

"I have several significant speeches over the next two months and am developing a new narrative that includes challenging the audience (depends on audience of course) to help with the cybersecurity problem. This doesn't mean specifically help DHS, although that might be included, but big issues that young and old, hacker or non-technical, could participate in and help the global problem. Once we develop the general framework of a speech, we could use it, or portions of it, as each of us do our DHS outreach and it would go a long way to developing common themes and talking points."

In this reviewer's qualified opinion and pursuant to Mr. Tom Baer's request, the following is a list of my comments and responses to Mr. Mark Weatherford's request.

2.0 Comments

Challenge 1: The Cybersecurity threats to systems supporting Government, Industry, academic, and private citizens, on critical infrastructures, are evolving and growing.

Comments on Challenge 1: The interdependency and interconnectivity among information systems, the Internet, and other infrastructures can amplify the impact of intruders' threats that have potentially impaired operations of critical Internet-based systems, the viability of sensitive information, and the flow of commerce. Furthermore, the high-technology network's reliance on Information Technology (IT), utilizing Cloud Computing Technology (CCT), through Internet-based systems have significantly exposed the telecommunications Cybersecurity environment and resulted in unknown vulnerabilities. Unfortunately, this reliance has been severely exploited by attackers and caused potential vulnerabilities that have not yet been exploited by attackers.

Solutions to Challenge 1: As the GAO reported in January 2011, securing smart grid systems and networks presented a number of key challenges that required attention by Government and Industry. These included:

- Development of a coordinated approach to help monitor Government, Industry, and private citizens' compliance with voluntary standards. These standards should support the Federal Energy Regulatory Commission (FERC) effort that is responsible for regulating key aspects of the electric power industry, which includes adopting Cybersecurity and other standards it deems necessary to ensure smart Internet-based network functionality and interoperability.
- Development of a Cybersecurity network to help build into a high-technology Internet Cloud-based system devices. High-technology Cloud-based systems should be developed with strong security architecture and multi-layered security features. The Government should set standards, at a minimum, and provide support to Industry and private citizens when it is required.
- Development of an efficient and effective centralized information-sharing Cloud-based mechanism that is fully capable of providing Cybersecurity information to Government, Industry, and private citizens. This Cloud-based mechanism should utilize and enhance the existing Government and Industry information sharing systems and research and development centers in a safe and secure way.
- Development of a set of cost effective standards, best practices, and metrics for evaluating Cybersecurity threats, intrusions, and information sharing among Government, Industry, and private citizens.

Challenge 2: Although most of the Government and Industry Cybersecurity officials are proactively complying with the Federal Information Security Management Act (FISMA), still there is an urgent need to certify their IT security systems and encrypt their data. These officials are openly and privately stating that the security of the United States is still vulnerable to intrusions and commerce could be adversely impacted in the future.

Comments on Challenge 2: The primary reason behind Government and Industry Cybersecurity vulnerabilities is that the number of threats to the nation's infrastructures and commerce has significantly increased due to intrusions nationally and internationally. In addition, the Cybersecurity threats to our Internet-based systems have grown far more sophisticated and complex in recent years, outflanking and maneuvering traditional rigid and inflexible Government and Industry security entities.

Solutions to Challenge 2: As the Government debates its appropriate role in Federal, Industry, and private-sector Cybersecurity activities, we have to realize that it is already responsible for securing its own networks and information. This is challenging and expensive but the cost is far less than that of compromised systems. Many of the recent Cybersecurity technologies developed and utilized by Government and Industry are applicable to Federal components as well as Industry and private citizens. While our nation's defense and intelligence communities are safeguarding our infrastructures and preventing intrusions to Internet-based networks that could damage, steal, and corrupt our sensitive information, we should be vigilant in our efforts to upgrade our systems continuously. The 21st Century United States CCT relies on information technology systems and networks to control our commerce through institutional common means such as emails and data sharing. Government acknowledges that we need to take actions to adapt and upgrade modern technologies and to prevent intruders' from accessing and damaging our vital systems.

Challenge 3: The next Pearl Harbor will be a cyber attack crippling our Government components and commerce.

Comments on Challenge 3: Government should build partnerships between Federal needs, academic research, and industry solutions to protect our information and critical Internet-based infrastructures. The Government should also bring together businesses and regional research and development partners to harness the talents and creativity of subject matter experts (SMEs). In addition, it should incorporate the perspec-

tives of public and private entities to build a competitive cyber workforce that meets our 21st Century national security short-term and long-term objectives. Government, therefore, should engage all of our states' educational institutions, businesses and other invested partners in a common goal of attracting the best SMEs and training the most advanced technologists to fulfill our national Cybersecurity goals.

Solutions to Challenge 3: Perhaps the most significant changes in our culture have been through the use of Internet in our daily lives. The profound effect of Internet-based technologies has enabled us to access our bank accounts on our computers and to connect to social networks from our phones. The Internet technology proliferation and expansion has impacted all aspects of our lives and will continue influencing our decisions for decades to come. This is a paradigm shift in our way of life, culture, and thinking; however, the consequences are that serious new Cybersecurity vulnerabilities have also emerged. To safeguard our nation's intellectual property and commerce, Government needs to offer more assistance to private owners of our critical Internet-based infrastructures and .com networks.

Challenge 4: The challenge and dilemma confronting Government is how to defend critical systems while protecting our civil liberties and privacy.

Comments on Challenge 4: We need legislation to bring our nation in line with the technological realities facing us through the Internet and online communications systems. We also need to pass laws and legislations that would protect our critical infrastructures and safeguard our civil liberties because protecting our nation's infrastructures is also safeguarding personal identity and liberties of our citizens. We need to bring together Government, Industry and academic partners to harness the talent and creativity of SMEs to build a framework and then incorporate the perspectives of public and private entities to build a competitive cyber workforce that meets our national security needs. While building the Cyber workforce, Government must educate the country to define the balance of defending our critical infrastructures and protecting our civil liberties and privacy. In order to strengthen the pipeline for these efforts, Government should engage all of our states' higher-education, businesses, research and development centers, and other invested partners in a common Cybersecurity goal to keep our nation and civil liberties safe from those who intend to harm us.

Solutions to Challenge 4: Government needs to establish a technical Cybersecurity roadmap towards an enterprise services "platform." To date, the most prevalent cyber threat has been exploitation of our networks. By that, we refer to the theft of information and data from Government and commercial impacts as well as other disruptions:

- Government impact: Foreign intelligence services have exfiltrated military plans and weapons systems designs.
- Commercial impact: Valuable source codes and intellectual properties have been stolen from Industry, research and development centers, and academic institutions.
- Internet impact: Disruption of our networks by adversaries seeking to deny or degrade the use of important Government, commercial, and private networks.
- Cyber-based impact: The most dangerous Cybersecurity threat confronting our nation is cyber-based destructions, where sophisticated technologies are used to cause physical damage to our Government, Industry, and private citizens.

Challenge 5: Cybersecurity challenges, solutions, and path forward.

Comments on Challenge 5: Following is a list of the Government's proactive Cybersecurity initiatives:

- Government will formally recognize Cyberspace as a new operational domain—like land, air, sea and space. Treating Cyberspace as a domain means that the military needs to operate and defend the United States networks, which is why we have established the U.S. Cyber Command, housed at Ft. Meade.
- Government will formally equip our networks with active defenses. We have developed and now employed a more proactive and effective approach to cyber defense that operates at network speed, using sensors, software, and signatures derived from intelligence to detect and stop malicious codes before they succeed.
- Government will formally ensure that the critical infrastructures are protected on which our Federal components, Industry, and private citizens can securely depend.
- Government will formally build collective Cybersecurity defenses with our allies linked to their cyber-based defenses to provide information sharing and prevent intrusion attacks.
- Government will coordinate our nation's vast technological and human resources to ensure that we retain our preeminent capabilities in Cyberspace, as it does in other high-technology domains.

The President's Cyberspace Policy Review identifies 10 near term actions to support our Cybersecurity strategy:

1. Appoint a Cybersecurity policy official responsible for coordinating the Nation's Cybersecurity policies and activities.
2. Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure.
3. Designate Cybersecurity as one of the President's key management priorities and establish performance metrics
4. Designate a privacy and civil liberties official to the NSC Cybersecurity directorate.
5. Conduct interagency-cleared legal analyses of priority Cybersecurity-related issues.
6. Initiate a national awareness and education campaign to promote Cybersecurity.
7. Develop an international Cybersecurity policy framework and strengthen our international partnerships.
8. Prepare a Cybersecurity incident response plan and initiate a dialog to enhance public-private partnerships.
9. Develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure.
10. Build a Cybersecurity-based identity management vision and strategy, leveraging privacy-enhancing technologies for the Nation.

Solutions to Challenge 5: To satisfy the challenges identified above, Government will provide the following Cybersecurity solutions safeguarding its components, Industry, and private citizens' information infrastructures:

- Government will formally enforce and define its Cybersecurity policies: Prioritize risks and define requirements that govern our Industry, and private citizens. It will also enforce these policies through built-in high-technology automation and workflow.
- Government will support Industry Cybersecurity needs by proactively taking an information-centric approach to safeguard knowledge-based accessibility and accuracy. It will also initiate a content-aware approach to protecting information that is the primary solution to defining, identifying, and classifying confidential and sensitive information. This information-centric technology will identify where sensitive information resides, tracks individuals accessing it, and monitors its flow through various Internet-based systems. In addition, it identifies and records who has accessed it and how it was accessed and departed through various hardware, software, and interface vehicles. Furthermore, the information-centric system effectively encrypts various endpoints to help Cybersecurity officials minimize the consequences associated with lost devices and intrusions.
- Government will help Cybersecurity access control to identify, validate, and protect the legitimate users and prevent intruders from damaging nation's systems.
- Government will create a Cybersecurity environment and implement security procedures that distribute and enforce patch levels, automate processes to streamline efficiency, and monitor and report network systems' status.
- Government will protect its infrastructures as well as Industry and private citizen network systems by safeguarding United States systems' endpoints that include all of the Internet-based communications networks. Furthermore, it will initiate legislation, policies, and procedures that effectively protect critical internal servers, routers, and other key systems' components. It will also support the capability to store and access sensitive information and the ability to back up and recover classified and unclassified information in cases of data pollutions, damages, and intrusions.

ABOUT THE AUTHOR

Currently Dr. Ghahramani is a member of the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC). Before joining the DHS, he was the Chief Technology Officer (CTO) of Eurpa Telecommunications and General Dynamics Lead Scientist before that.

Dr. Ghahramani was the Founder and Chairman of the Board of MewsTech, Inc. and BG Technical Management Solutions, Inc. Prior to starting his two successful companies, he was a distinguished member of Technical Staff (DMTS) at the AT&T Bell Laboratories and generated more than $1.9B in funded projects with various countries, industries, and governments. His extensive work also includes projects with Sandia Laboratories, Livermore National Laboratories, and Oakridge National Laboratories, incorporating sensor and telecommunications technologies. His work experience covers several years in government, academia, industry, and consulting. Dr. Ghahramani has presented and published numerous referred papers; and has been an active participant and officer in several national and international organizations and honor societies. He holds eleven patents in addition to two international patents. Dr. Ghahramani received his Ph.D. in Industrial Engineering from Louisiana Tech University; MBA in Information Systems from Louisiana State University; MS in Applied Mathematics and Computer Science from Southern University; MS in Industrial Engineering from Texas Tech University; and BS in Industrial Engineering and Management from Oklahoma State University.

Dr. Bahador Ghahramani, P.E., CISM, CPE
Department of Homeland Security
Headquarters
US-CERT Communications
Office: 703-235-3056
Mobile: 571-340-1841
Fax: 703.235.5963
E-mail: bahador.ghahramani@hq.dhs.gov
E-mail: bahador.ghahramani@us-cert.gov
Website: <http://www.us-cert.gov/>