World Applied Sciences Journal 31 (4): 559-561, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.31.04.14325

American Political Experts on Cyber Security

Darya Sukhovey and Olga Miroshnichenko

School of law, Far Eastern Federal University, Vladivostok, Russia

Abstract: The survey is devoted to the cyber security issue, a relatively new phenomenon which appeared due to computer and IT technology breakthrough at the end of the 20th century. The special attention was paid to different interpretations of the concept of cyber security and cyber threat as developed in the works of American political scientists. The analysis of arguments in favor of the cyber threat existence is based on the literature published after 9/11.

Key words: Cyber Security · Cyber Threat · American Political Scientists · Drones

INTRODUCTION

Mankind has stepped into the third millennium with maximum convenience. Revolution in the sphere of technology gave us an opportunity to use a variety of gadgets that twenty years ago could have been seen only in fantastic films. Nowadays not only trillions of different questions are being arranged via mobile phone, countless amounts of documents are being sent through the internet, millions of people go through effective treatment due to significant developments in medicine instrumentation people are going through effective treatment; outer space devices guarantee aircraft and marine navigation. All these modern innovations made society extremely more dependent on the IT industry. And it is clear that this IT based society is quite vulnerable to outside interference or damage, which becomes unavoidable as the majority of technological devices are comprised with different cyber components. Certainly every threat requires adequate protection. Thus it is important to know whether the states consider cyber security to be a point for special concern and what measures are undertaken by the states in response to the threat. In this regards the position of the United States of America is highly important as this sole superpower is often considered to be far from being the most peaceful realm in the world. To know beforehand what the US Government considers to be a threat that which would be eliminated in the nearest future next time is not a useless piece of information for each player on the world arena.

As the US Government is influenced a lot by political academic society and is acting in close collaboration with it we pursue a goal to describe in this survey the considerations of American political experts on the cyber threat problems. Knowing tendencies in leading think-tanks and analytical centers of the USA we can predict the US Government general policy and possible measures and actions in the sphere of cyber security. But practices of leading think-tank analytics as the Brookings Institution and the Council of foreign relations were the sources of our survey.

Cyber Threat Proponents: Detailed review of cyber threat issue is contained in the US Defense science board task force report "Resilient military systems and the advanced cyber threat". After conducting an 18-month study the Task Force concluded that "the cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War" [1].

The Task force concluded that "network connectivity that the United States has used to tremendous advantage, economically and militarily, over the past 20 years has made the country more vulnerable than ever to cyber attacks" [2]. Experts underline different levels of the threat:

Corresponding Author: Darya Sukhovey, School of law, Far Eastern Federal University, Vladivostok, Russia.
Tel: +147065409.

- Tiers I and II attackers primarily exploit known vulnerabilities
- Tiers III and IV attackers are better funded and have a level of expertise and sophistication sufficient to discover new vulnerabilities in systems and to exploit them.
- Tiers V and VI attackers can invest large amounts of money (billions) and time (years) to actually create vulnerabilities in systems, including systems that are otherwise strongly protected.

Experts note that threat represented by V and VI tiers is "such magnitude and sophistication that it could not be defended against. As such, a defense-only strategy against this threat is insufficient to protect U.S. national interests and is impossible to execute. Therefore, a successful DoD cyber strategy must include a deterrence component. One key element of deterrence is the believable military capability to either defeat an attack or to provide a survivable response that holds at risk something the adversary highly values (*i.e*. the adversary's cost exceeds the adversary's gains). The top of that escalation ladder is the present U.S. nuclear deterrent" [3]. Thus nuclear answer to cyber threat is not excluded by American political experts. Michel Mazza in his speech in front of the House Foreign Affairs Committee's Subcommittee on Europe, Eurasia and Emerging Threats touched upon the question of Chinese cyber threat attack. The author is confident that "United States should be clear about how it will respond to the use of strategic cyber weapons on American soil" and advises the Department of Defense to "explore whether it is possible to conduct cyber exercises that will effectively demonstrate U.S. capabilities, much as conventional exercises are used, for example, to deter North Korea…U.S. military could set up an allied public training exercise in which it conducted cyber-attacks against a 'Country X' to disable its military infrastructure such as radars, satellites and computer-based command-and-control systems" [4].

Another point of view can be found in the work of Darrell West "Vision for homeland security in the year 2025". The author notes that "nation-states represent the most sophistical cyber capabilities with the greatest potential to undermine our military and economic advantages and threaten critical infrastructure and key functions" [5]; thus he considers that sates are not the only actors in this field and the threat is coming from "non-state actors" in the form of individuals and groups have a wide range of capabilities and intentions" [6].

John Villasenor stepped forward in theoretical thinking on the topic: he pays special attention to the threat of drones attacks to the security of the US. The author considers that "it is only a matter of time before rogue groups or nations hostile to the United States are able to build or acquire their own drones and to use them to launch attacks on our soil or on our soldiers abroad" [7]. Proposed Solutions to the national security risks posed by drones in the wrong hands include "1) measures designed to make it as difficult as possible for rogue groups to obtain drones and 2) steps aimed at stopping or minimizing the harm due to attempted drone attacks on American interests" [8].

CONCLUSION

Cyber threat has become one of the key issues in American political discourse and all the authors agree that the threat demands for a clear preventive strategy. There is an open question in American political scientific society about military response to cyber threat. The first question is who should be punished for attack: the state or individuals? Another one is: what concrete measures should be taken. Despite there are some controversies questions it is clear that American political experts do not exclude the possibility of use of force as an answer on cyber-attack. Taking into consideration that American academics are working in close cooperation with political leaders that means the provisions for American military response are extending.

REFERENCES

1. Task force report: resilient military systems and the advanced cyber threat, 2013. Department of defense science board, January, retrieved from: http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf
2. Ibid
3. Ibid
4. Mazza, M., 2013. Testimony before the house foreign affairs committee's subcommittee on Europe, Eurasia and Emerging Threats, Foreign affairs committee, March 21, retrieved from: http://www.aei.org/speech/foreign-and-defense-policy/defense/cyber-attacks-an-unprecedented-threat-to-us-national-security/
5. Ibid
6. West, D.A., 2012. Vision for homeland security in the year 2025. Brookings institution, June 26, retrieved from: http://www.brookings.edu/research/papers/2012/06/26-security-homeland-west

7. Villasenor, J., 2011. Cyber-physical attacks and drone strikes: the next homeland security threat, July 5, retrieved from: http://www.brookings.edu/research/papers/2011/07/05-drones-villasenor
8. Ibid