The US Cyber Strategy

Edward Gauvin

Roger Williams University

Cyber security is one of the main challenges different countries face in the technology sphere. This is ue to the United Stated having made an initiative of investing heavily in the cyber security domain. This is being training and ensuring that they have the best cyber security brains and technologies. Cyber wars have been conducted by non-state and state parties who are aiming at knowing the extent that the U.S government can withstand in terms of cyber-attacks. This may be aimed at disrupting organizations working environment to steal intellectual property and even disrupt military operations. Due to this, the U.S government came out with strategic goals that can be used to help in containing cyber-crime attacks.

One of the strategic goals is to build and maintain ready forces with the capability to conduct cyberspace operations. To achieve this, the U.S Department of Defense (DoD) had to come out with a Cyber Mission Force (CMF). Through CMF, cyber missions can be coordinated and done within that department. The U.S DoD had to improve in recruiting its personnel, enhancing the training and strongly relying on the private sector. The people in CMF group should work at becoming the bests since the training is so objective oriented. Recruitment should be advanced. This includes developing and enhancing their career. CMF's have a unique real training that will help the involved individuals. To enhance and build up their skills, DoD has negotiated with the private sector to include exchange programs so as to gain real experience. So, acquiring and building a strong cyber mission force is one of the U.S strategic goals.

The other strategic goals were to defend the DoD information network, secure DoD data. Moreover, mitigate risks to DoD. Through this, the DoD has planned to come up with a single network architecture. This will help in reinforcing security and easing network management. Under this, they have planned to assess the network and systems security together with designing risk mitigation strategies.

The third goal was to defend the Homeland and US vital interests from disruptive or destructive cyber-attacks of significant consequence. Under this, the Department of Defense has planned to work with the local with the private sector and local contractors to ensure one can pose a threat to then U.S government. The DoD must come up with a warning, intelligence and operational strategies that can be used to deter any further attacks.

The fourth goal aims at building and maintaining many cyber options and plan to use these options to establish control during conflict escalation and to shape the conflict environment at all stages. This can be achieved by the president and the DoD being allowed to have full control of cyber security at all times. This means the military should be capable of disrupting systems and networks all the times if authorized to do.

The last strategic goal is to maintain robust international alliances and partnerships to deter shared threats and increase international security and stability. To achieve this, a partnership should be created between the DoD and the corporate companies. This is because the companies have a great talent in serving cyber security issues.

There are key factors that should be considered during implementation. This calls for priorities in implementation. There is the most important thing that should be implemented in the strategy before anything else. Building a strong cyber workforce is so essential for such a mission. This will help ensure that the country is always secure and ready since there is a team specialized in undertaking such operation.

This can be categorized into different forms. Maintaining a persistent and vigorous training can help in building a strong workforce. This will be a kind of training with collective goals and strategized to meet future operational goals. Career development is also vital in this. After the training, the workforce needs to enter into areas of specialization that will sharpen their skills in their direction of work. Through a consistent career development plan, the DoD can produce the best cyber workforce.

The development and implementation of exchange programs between the cyber workforce and private sector companies can assist in developing competent cyber warriors. To supplement what they have been taught, there should be a blend of what happens in the real world. This can be achieved by allowing the workforce learn from the key cyber security leaders in the world. This will bring skill competency making the workforce more equipped. The DoD's plan to develop a national initiative for cyberspace education can be of great significance. Integrating learning institutions in the cyber workforce plan can be a great idea that can put talent into practice ("The Department of Defense Cyber Strategy", 2016).

The US has certain strengths that put the in the front when matters of technology are to be handled. The US is known for its prowess in technology. This is one of their strengths in relevance to the implementation of cyber security strategy. The US has come up with the most impressive technologies including simulations. This proves that it is valid that they will still head in the cyber security domain.

The US has the best high-tech companies in the world. This has been led by the deepened research in the US. They are the core inventors of the networks, and this means that they have the most cutting edge technologies. If this is the case, their companies are producing the most high-end devices in the field of computing. This means that their strategy is viable since they have the businesses to give advice on the best security measures and strategies.

Research institutions have contributed significantly in the field of technology. The US being a country that host the Ivy League universities has an added advantage in its plan towards the implementation of their cyber security strategy. Having a high level of training institution can be one way to catalyze the project since it involves a lot of technological bits.

The economic status of the US is among the moving factors of this project. This is because the implementation, planning execution and maintenance of all the cyber security infrastructure heavily rely on capital ("Wired World: Cyber Security and the US Economy: Statement of Frank J. Cilluffo", 2016). With all these strengths, US has all the reasons to roll out its project in securing the borderless computing world.

The United States may have all the capabilities to implement their project but in every project, there lays a certain amount of risk. This happens to be weaknesses that the US DoD cannot be able to cover as they roll out their plan. One of the greatest risks is the parties involved or the project stakeholders. Bearing that the (DoD) handles weighty matters, it can be a great risk to involve third parties who may, later on, use the information acquired in the country.

For security companies that will be working together with the US DoD, there is a great risk that acquires(?) may learn secret information during the process. This may be even processed that govern how information is shared or how information flows in the department. If this is known, then the companies may act against DoD in some way indulging the authorities in a pool of integrity and confidentiality problems. The companies as a third party body for the project pose a great risk to the cyber security program, and this happens to be a weakness.

The institution or students who are involved in the project or the learning institutions may also lead to integrity and confidentiality compromise. Training them the operating procedures for securing the systems can lead to integrity and security compromise. This calls for well-strategized mechanisms of controlling how things should be done so as to avoid security compromise.

If the strategy follows the laid out plan, then chances are the US cyber security strategy will go through. This is because, from the feasibility study done on the US, all the tools and knowledge required for the strategy implementation are available.

Considering the knowledge for implementation, the US hosts the best computing brains, and it is the center of technology innovations. This means that the DoD will obtain information and know-how regarding the project from its citizens.

In the private sector, US has got competitive companies that can help in realizing the plan. By involving this techno savvy companies then, the strategy implementation will be easy. The US is also known for a stable economy. The economy is the driver for any success of a country. The economic stability of this country will see it through in achieving its dream towards cyber security dependency.

Although there may be no clear role for the US government to involve itself in cyber security issues, there is a great reason for the government to strategize and involve itself with the project ("A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace", 2013). Many threats that the US faces required proper and strategized approached to contain their severity. The threats are daunting, and if they are not properly addressed, then the US government may find itself in a pool of problems. This means that the government should invest a lot in strategizing and securing the government's property in the cyberspace.

**References**

A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace. (2013). The Heritage Foundation. Retrieved 27 March 2016, from http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace.

Wired World: Cyber Security and the US Economy: Statement of Frank J. Cilluffo. (2016). Fas.org. Retrieved 27 March 2016, from http://fas.org/irp/congress/2001\_hr/062101\_cilluffo.html

The Department of Defense Cyber Strategy. (2016). Retrieved 27 March 2016, from http://www.defense.gov/Portals/1/features/2015/0415\_cyber-strategy/Final\_2015\_DoD\_CYBER\_STRATEGY\_for\_web.pdf

.