**Cyber-Intrusions and Cyber-Terrorism**:

Non-negligible Cyber-Terrorism

Senqi Lin

University of Windsor

Non-negligible Cyber-Terrorism

**Introduction:**

With the development of [science and technology](http://www.baidu.com/link?url=Aa7j1gi5rwNvI5h1bGV2QazaIGMyLib5GMCyOOgVv5g1O3GCKlETktz1jYctqEEB5bKwBcM6TDQzTZvWHvsuKbdgTVbtQM5DWPmCKqAUngGux38RtciTCD0B4YXeqTCG" \t "https://www.baidu.com/_blank), terrorism is no longer a mere form of violence. Cyber crime is on the stage of history as a new form of terrorism, and those activities fully use the network as a tool and weapon that has highly intelligent and uncontrollable features.Network terrorism become a new potential threat to national multifaceted security,such polity, military and economy. For preventing and stopping cyber terrorism, we must recognize and attach importance to cyber terrorism. As the article from book *Readings and Cases in Information Security* has mentioned that the definition of cyber terrorism ,its features and how nation responds it, etc. In any case, prevention of cyber terrorism has become an important part of the national security system, and it is also the war without gun-smoke.

In the article , it has mentioned that the cyber terrorism can be generically defined as using network technology to engage in activity that can undermine a society’s ability which maintain internal or external orders. For example, it lists that someone launched DDoS attacks that effectively shut down websites. Thus, The FBI Director Louis Freesh admitted the threat is really exist and prevention of cyber terriorism is not negligible at modern age. But,the author, Whitman and Mattord give some suggestions from multiple aspects for solving the problem which is how to improve the national security to prevent the damage of cyber terrorism.

**Improve National Security**

Comparing with individual network crime, the cyber terrorism usually is caused by the otherness of political or religious perception. Thus, we need to take concern from multifaceted national security. Generally, cyber terrorism is in the interface of attack to pass the national system based on the fallibility of a security system. Ozeren states that the vulnerabilities to cyber terrrorism have four aspects.

First , advanced technology is one of the most indispensable part for national security. Since there are various waysto gain access to information in cyberspace, it is certain that terrorists and their supporters have been engaging in extensive activities and they will continue to do so. For dealing with this kind of problem, he lists that use multiple actions to guarantee the security of information, isolate crucial resource form internet and utilize encryption technology.Second, imperfect law is also one of the vulnerabilities for cyber terrorism to utilize. For improving the effectiveness of law, we should clearly define a cyber attack and rational punishment to the different intensity of cases. Moreover, the source of cyber attack may come form inside or outside of country.Thus, how to make the anti-terrorism strategies to become consistent is also rough problem for each country.Third, the conflict of cultural might be one of the reasons to cause the consequence of cyber terrorism.Furthermore , some of countries do not take the corporate responsibility to cyber terrorism that is also one of tricky factors.Fourth, the attack of cyber terrorism may also based on a country’s relative position in the world to influence the balance of world polity.

Even though Ozeren represent those weakness of nation for cyber terrorism, but I think we should attach important to the education as the first. We all know that suppressing the spread of terrorist forces is temporarily,and we can not fundamentally eliminate terrorism source in short time.Therefore, it is important that to establish the correct cognition to the world while growing up.Meanwhile, participating actively with the anti-cyber terrorism intentional strategy is one of ways to reduce the conflict of perceptions to cyber terrorism with other nation.

**The Risk of Terrorism**

As the early 19th century, United States realized the dangerous of cyber threat and started to establish the basic security system for preventing. In May 1998, Clinton signed the Presidential Decree No. 63 on the Protection of Critical Infrastructure in the United States [7], which for the first time defined the concept, significance and security of information security, and established key infrastructure safeguards Office, and called for "to take all necessary measures to quickly eliminate the obvious weaknesses that led to physical and cyber attacks on key infrastructures." In January 2000, Clinton issued the National System for Information System Protection, establishing the United States to prevent cyber crime,which is the basic framework of cyberspace security system nowadays.

On February 14, 2003, the United States announced the world's first national strategy to fight against terrorist attacks - the National Strategy to Secure Cyberspace, threatening and vulnerable to US cyberspace And clarified the guidelines for maintaining cyberspace security, and put forward five priority development goals and 47 action proposals [9]. The strategy serves as a guiding document for the maintenance of cyber security in the United States, which indicates the direction of action by governments, private enterprises and institutions, and ordinary citizens in improving cyber security. At this point, the United States anti-cyber terrorism strategy initially formed.

There are many advanced places in the United States to guard against cyber terrorism, which is worth learning to us, but there also left some questions that we need to be concerned.Debate on privacy issues, In the United States to strengthen network security at the same time, the US government departments continue to legal and behavior to achieve the Internet service providers and users of the right to intervene, in particular, information security monitoring and inspection, such as the anti-terrorism departments have implemented data mining Data Mining project, the US people fear that the use of this technology will pose a threat to citizens' rights such as privacy, so the United States

Will have to pass the bill to limit the implementation of the project. The Department of Defiance's "Total Information Awareness project" was launched ambitiously in 2003, trying to build a giant database to collect and analyse any data of possible terrorists, and finally because of the civil rights and personal Privacy, and was forced to suspend. The Patriot Act, which has been authorized by the Anti-Terrorist Department to monitor the public, has allowed the law enforcement agencies to eavesdrop on the telephone of terror suspects and track the use of their Internet and e-mail, which has sparked a national debate. The United States government in the fight against cyber terrorism on a series of practices gradually more and more people feel the application of the Internet inconvenience and surveillance. Therefore, more and more people ask the government to respect the privacy of individuals and reduce the network of individuals monitor. In the future, disputing over the right to freedom, privacy and national security will still continue.

Network security system is too large. Although the US network security sector construction is very complete, improve the prevention of United States to cyber attacks and cybercrime with a great significance effect. The US network security system is too large, so that efficiency issues are increasingly aroused people's attention.

**The difference of Canada**

Jennifer W. mentioned that U.S. government passed Uniting and Strengthening America by *Providing Appropriate Tools Reacquire to intercept and Obstruct Terrorism Act*, which simplify as PATRIOT Act after the 9/11 happened. Meanwhile,Canada also publish the Anti-terrorism Act to response to the event of 11 September 2001.Comparing those act between United States and Canada, the listing process from United States is less formal than Canada law and it did not introduce new offences designed to discourage, deter or prohibit people form dealing with terrorist property since United States has already support some recourse or have the relationship of trade cooperation to terrorists before they publish PATRIOT.

**The protections form Canada**

In 1996, the federal government recognized that systems that were critical to the operation of key infrastructure in Canada could be attacked by the network and that the government could play a role in protecting such systems from such attacks. In 1999, the Senate Security and Intelligence Committee's report recommended that the Government take action to review its ability to assess and reduce infrastructure vulnerabilities and to prevent or respond to physical and cyber attacks.

In 2000, the Government of Canada established a key working group on infrastructure protection to advise ministers on the role of the federal government in protecting Canada's key infrastructure. The Task Force has found that the limited security of critical infrastructure in Canada and the interdependent and interdependent nature of the interdepartmental, interregional, national and international borders at the provincial, regional and international levels need to strengthen the national strategy of security.

Governments have the capacity to provide national and international network security threats to key infrastructure owners and operators because they have access to sources of information that are not available to other stakeholders, such as sources of foreign intelligence. It can collect and share network threat information in a way that protects information sources and can use established partners to quickly notify all stakeholders.

In response to the concerns of the key Infrastructure Protection Working Group, the Government of Canada established the Key Infrastructure Protection and Emergency Preparedness Office (OCIPEP) in 2001. OCIPEP's mission is to develop and implement a comprehensive approach to protecting partnerships for key infrastructure in Canada, monitoring and analyzing cyber attacks and threats to federal systems.

In December 2003, the Government announced the inclusion of OCIPEP in the newly established Canadian public security department to integrate emergency operations and to work with operators at provincial, regional and private sector owners and key infrastructure. Figure 3.2 details the timetable of the federal government's commitment to protecting Canada's key infrastructure, including protecting the network threat.

**Conclusion**

Nowadays, the importance of the prevention of cyber terrorism can not be ignored. The network provide us with the convenience, but also provide a criminal short-cut for the terrorists. At present, terrorists want to led to a panic through network has a variety of difficulties, but once thing happened, the result can not be remedied and we can not bear it.

**Reference**

Michael E. & Herbert J. *Readings and cases in formation Security Law and Ethics*

Retrieved form:

<https://blackboard.uwindsor.ca/bbcswebdav/pid-590588-dt-content-rid-3201244_1/courses/0360305-91-2017S/Assignment%202%20Reading.pdf>

Jennifer W. *The USA PATRIOT Act And CANADA'S Anti-Terrorism Act:  
Key Difference In Legislate Approach*

Retrieved form:

<https://lop.parl.ca/content/lop/ResearchPublications/prb0583-e.htm>

The Report of the Special Senate Committee on Security and Intelligence.(2012, July 17).*Protecting Canadian Critical Infrastructure Against Cyber Threat.*

Retrieved from:

*<http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html>*