*Vytautas Butrimas*[*]
*The Ministry of National Defense of the Republic of Lithuania*[**]

# National Security and International Policy Challenges in a Post *Stuxnet* World

The international community has focused too much on addressing cybercrime and cyber hacktivist questions. The list of usual suspects responsible for cyber incidents associated with attacks involving the theft of intellectual property, sensitive private data, money and disruption of web services unfortunately has grown beyond the attention seeking student hacker, cybercriminal or social hacktivist. The public appearance of the *Stuxnet* family of malware designed to destroy specifically targeted critical infrastructure components in June of 2010 gave perhaps the first indication that States have entered cyberspace as one of the perpetrators of malicious cyber activity. The problem of States actively preparing and executing cyber-attacks against the critical infrastructures of other States has been largely ignored by the international community. These attacks raise national security issues concerning threats to the economic and social well-being of States. However the pervasive presence of cyber space as the common environment where all modern industrial processes take place and the interrelations developed among the critical infrastructure of other States raise cross-border security issues as well. The international community must act in order to insure that the use of this new weapon by States will not get out of hand and be the cause of new and more serious international conflicts. Three solutions and a possible model are proposed to manage this disruptive activity of States in cyberspace at the international level.

## Introduction

Closely interwoven within the domains where human action take place is the invisible yet pervasive domain of electromagnetic activity supported by information and communications technologies called cyber-space. In this environment systems and processes comprising the modern systems of finance, energy, transportation, and telecommunications have developed based upon the capabilities of these new dynamic technologies. These systems have grown into complex and interrelated infrastructures and processes that are critical to the functioning of modern societies and economies.

[*] *Vytautas Butrimas* is a Chief Advisor for Cyber Security of the Ministry of National Defence of the Republic of Lithuania. Address for correspondence: Totorių 25/3, LT-01121 Vilnius, Lithuania, tel. +370-5-2735775, e-mail: vytautas.butrimas@kam.lt

[**] Evaluations and ideas presented in this article exclusively belong to the author and can never be considered an official position of the Ministry of National Defense of the Republic of Lithuania or its departments.

DOI: 10.2478/lasr-2014-0001

Together with these new capabilities there are also new vulnerabilities. Hostile actors with knowledge of these vulnerabilities can execute cyber-attacks that can not only disrupt a critical service or industrial process but even result in loss of life. To the extent that cyber-attacks disrupt the processes and services of these critical infrastructures is the extent to which they are national and international security issues. A cyber-attack on the telecommunications information infrastructure used by the financial system could impose severe stress on society and cause a serious crisis for any government. Imagine that for a week people were denied the use of their credit cards or the ability to make other electronic transactions. How long could we live from our wallets if supermarkets and gas stations suddenly took payment in cash only (as happened in Cyprus when its Government ordered bank closures in the spring of 2013)?[1] Think about what would happen if power station, gas pipeline and/or railroad control center operators suddenly lost their view of and ability to control a critical process? Such events have happened and have caused loss of life.

In the last ten years the main sources of malicious cyber activities and threats in cyberspace have been cyber criminals and computer hacker-hacktivists. For the most part dealing with these malicious cyberspace actors has been left to law enforcement. Recent high profile arrests of these individuals and small criminal groups have been made thanks to coordinated domestic and international law enforcement efforts.[2] The international community for the most part tends to understand cyber security in terms of cybercrime or "cyber terrorism". One good example is the Council of Europe's Cybercrime or "Budapest" Convention[3]. Another example is the recently published Guide on protecting critical energy infrastructure from terrorist threats emanating from cyberspace.[4] The OSCE recognized that the "disruption or destruction of this infrastructure [by terrorists] would have serious impact on the security, safety, economic well-being and health of individuals and the world as a whole."[5] However, the question remains of whether terrorists are the only threat actors

[1] Steininger M., "What's behind the bailout crisis in Cyprus?", *Christian Science Monitor*, http://www.csmonitor.com/World/Europe/2013/0329/What-s-behind-the-bailout-crisis-in-Cyprus , 29 03 2013

[2] Gilbert D., "Dutch Suspect Sven Olaf Kamphuis Arrested for Biggest Cyber Attack in Internet History", *International Business Times*, http://www.ibtimes.co.uk/articles/461848/20130426/spamhaus-suspect-arrests-spain-kamphuis.htm, 26 04 2013.

[3] Council of Europe, *Convention on Cybercrime*, 23 11 2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm,

[4] Organisation for Security and Cooperation in Europe, *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace*, 2013, http://www.osce.org/atu/103500.

[5] Ibidem, p. 7.

that can use cyber weapons of mass destruction (WMD) to disrupt or destroy critical infrastructure. There is little evidence that "al-Qaeda" style terrorists are sitting down and planning a cyber-attack from a computer. They lack (so far) the skill sets, interest and capability to prepare and deploy complex cyber-weapons on their own. There is a third but less appreciated source of cyber threat to critical infrastructure.

In the past ten years the malicious cyber activities of states in cyberspace has become an issue that needs to be placed on the international security policy agenda. Cyber-attacks have evolved beyond the patriotic or politically motivated cyber riots that resulted in the temporary and non-destructive (in terms of data lost or damaged IT equipment) denial of services attacks on Estonian Government, banking and news portals in 2007. They have progressed since then to the use of cyber weapons that can destroy critical infrastructure. Examples include cyber-attacks directed at Iranian nuclear facilities starting in 2009, Saudi Arabia's oil industry in 2012, and against United States financial institutions in late 2012 and early 2013.

Reaction to these attacks by victim states in the absence of international action has led to the start of a cyber-arms race and even bellicose threats of retaliatory action.[6] International institutions tasked with promoting peace and international order have not arrived at a consensus on what to do. The problem will not go away because cyber-attacks directed at critical infrastructure are likely to have significant cross-border effects that could destabilize the international order. The difficulties in identifying the attacker and the relatively low cost in executing successful deniable attacks are now appreciated by nations. What new challenges does this malicious activity of states in cyberspace pose for international security policy making? What does the international community risk in not acting to address this problem? What can be done to manage this problem and reduce the potential for a cyber-attack escalating into a larger conflict? This article will discuss these questions and argue for more focused action by the international community to address the malicious cyber activity of states.

[6] Alexander D., „US reserves right to meet cyber attack with force", *Reuters*, http://www.reuters.com/article/2011/11/16/us-usa-defense-cybersecurity-idUSTRE7AF02Y20111116, 15 11 2011

## 1. States Become Cyberspace "Outlaws" in an Environment that Has No Cyberspace "Sheriffs"

In 2007 the malicious activities of states emerged as a new source of cyber threats on critical infrastructure. Much has already been written about the April 2007 denial of service (DOS) cyber-attacks directed at on-line Estonian Government and banking websites. It has been called the first cyber war[7] involving governments. Although these denials of service attacks were temporarily successful they caused no real lasting physical damage to computing equipment or information systems. The "Bronze Soldier" statue incident provided enough cause for an alliance of pro Russia cyber criminals and hacktivists to produce a cyber-riot. Even though it was not possible to prove, Estonians looked upon their neighbor Russia as responsible for the attacks. What is worth remembering is that Estonia was forced to disconnect (for a few hours) itself from the Internet. Nothing would better aid a potential aggressor's actions against a state than to cut off its victim's ability to communicate with the outside world.

Something more sinister may have occurred in cyberspace later that year. In September of 2007 the Israeli Air Force successfully penetrated Syrian airspace and bombed a suspected secret nuclear facility. This apparently easy penetration of airspace aroused the suspicion of some aviation experts[8]. Many asked how one of the most sophisticated air defense systems in the Middle East could fail to record or respond to a major violation of its airspace and bombing on its sovereign territory (Syrian air defense, by the way, had no problem in later detecting and shooting down a single Turkish jet flying over the Mediterranean[9])? Experts suggested that the Israeli military used a cyber-trick to confuse or disable Syrian air defense.[10] Former National Security Adviser Richard A. Clarke thought this explanation was plausible enough to put into his book as an example of cyber war.[11] The objective, however, was apparently met. A suspected nuclear facility was neutralized with little or

[7] Traynor I., „Russia accused of unleashing cyberwar to disable Estonia", *The Guardian*, http://www.theguardian.com/world/2007/may/17/topstories3.russia , 15 05 2007.

[8] Carroll W., „Israel's Cyber Shot at Syria", *Aviation Week*, http://defensetech.org/2007/11/26/israels-cyber-shot-at-syria, 26 11 2007.

[9] Burch J. „Pilot bodies from downed Turkish jet retrieved", *Reuters*, http://www.reuters.com/article/2012/07/05/us-syria-crisis-jet-bodies-idUSBRE8640KU20120705, 05 07 2012.

[10] Fulghum D., „Why Syria's Air Defenses Failed to Detect Israelis", *Aviation Week*, http://www.aviationweek.com/Blogs.aspx?plckBlogId=Blog:27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckPostId=Blog:27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post:2710d024-5eda-416c-b117-ae6d649146cd, 03 10 2007.

[11] Clarke R., *Cyber War*, Harper Collins, 2010, p. 7.

no collateral damage. Together with the Estonian cyber-attack, government sponsored malicious cyber activity could not be proven. However, the lessons learned about the effectiveness of such attacks and the lack of international response certainly were noticed by those who organized them and perhaps by others considering executing their own attacks.

While the attack on Syria aroused little sympathy it should be noted that air defense makes use of radar which is also used for managing civilian air traffic. Civilian aviation is part of the transportation infrastructure, the control systems of which are vulnerable to cyber incidents and attacks.

In August of 2008 a cyber-attack as a means to temporarily disrupt a nation's cyberspace took on a new and deadlier form – use of cyber-attacks simultaneously with a traditional military operation. It combined several elements used in the Estonian attack a year earlier: grass roots patriotism channeled with the help of social networks, professional botnet herders, elements of organized crime and suspected (but unproven) government support. The result was the execution of a well-planned, well timed and debilitating cyber-attack against Georgian government and civilian institution websites. This attack succeeded in cutting off (echoes of Estonia 2007) the Georgian government, its people and the world from on-line access to information about what was happening in the country. In short Georgia's ability to organize and coordinate its national defense was severely compromised. One study of the cyber-attack against Georgia suggested the appearance of a darker trend – the possibility for physical destruction of critical infrastructure components.[12] However, for some reason restraint was chosen by the perpetrators.[13] Other than some arrests made in Georgia there have been no actions by the international community to punish those behind these cyber-attacks. Again lessons were learned and reinforced – acting maliciously in cyberspace is an attractive option because no one will try to catch and punish you.

## 1.1. *Stuxnet*

By 2009 proof of the involvement of states in preparing and executing cyber-attacks still lacked a "smoking gun". That is, until the summer of 2010, when the first reports of a sophisticated "cyber weapon" designed to attack

[12] Bumgarner J., Scott B., „Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008.", *U.S. Cyber consequences Unit.*, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf, 2009, p. 5.

[13] Ibidem, p. 5.

critical infrastructure was reported to the cyber security community. The *Stuxnet* malware came as a surprise to many analysts. The most dangerous parts of *Stuxnet* from a technical point of view was that it interfered with the monitoring and control of processes taking place in complex industrial systems.[14] The malicious code of this cyber-weapon caused a "loss of view" and "loss of control" of machinery and associated industrial processes. It achieved this by intercepting and inserting false data sent to the operators telling them that systems were functioning normally when actually they were not. To put it more simply the effect was similar to what would happen to a driver of an automobile whose mechanisms were manipulated to direct him over a cliff. The driver feels no alarm or reason to take action since the view of the road he sees ahead is "normal". Even if he tried to take action to save himself he would find that he had no control of the steering wheel, brake pedal, and engine. *Stuxnet* is different in the sense that it did not attack Windows computers. It instead sought to destroy equipment used in a critical production process. It was not cybercrime, as no money apparently was made from it. The degree of technical skills and intelligence assets required in the preparation and delivery of this weapon to its intended target (nuclear enrichment facility in Iran) indicated the work of a State (for an understanding of *Stuxnet* and operation "Olympic Games" a good book to read is by David E. Sanger).[15]

The appearance of *Stuxnet* can be said to be the equivalent of a "Hiroshima moment" for cyber security and international relations in terms of changed mind sets. The first known execution of a cyber-attack by one state against the critical infrastructure of another state proved that the "gloves were off". It was recognized that this technology was now being applied to disrupt and destroy machinery and industrial processes. This operation which probably was politically motivated (keeping Iran from making the bomb) also introduced a new problem of cyber weapons coming into the hands of lesser skilled hacktivists, criminals and even terrorist groups[16]. *Stuxnet* code unfortunately made it to the Internet where it could be freely copied and analyzed. The methods could be studied and the code adapted to execute new and destructive cyber-attacks. Critical infrastructure (telecommunications, energy, financial, systems) which was up till then largely living in its own isolated world of closed communications networks and obscure proprietary

[14] Langner R., „Cracking Stuxnet: a 21st century cyber weapon", Ted Conferences, http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html, 03 2011.

[15] Sanger D., *Confront and Conceal*, Crown Publishers, New York, 2012, p. 504

[16] Simonite T., „Stuxnet Tricks Copied by Computer Criminals", *MIT Technology Review*, http://www.technologyreview.com/news/429173/stuxnet-tricks-copied-by-computer-criminals/, 19 09 2012.

technologies became a new area of interest for hackers. Not merely governments could seek ways to exploit newly exposed vulnerabilities and do physical harm to industrial control systems (ICS) of national critical infrastructures. For the first time it was plausible to think about the possibilities of true cyber terrorism. This technology was now available to terrorists groups lacking the skills to develop their own cyber WMD. *Stuxnet* once again further reinforced the lessons learned from earlier cyber-attacks. The apparent success of the operation contributed to not only new recognition of the vulnerability of critical infrastructures, it also provided the international security policy community a new problem: what to do about States playing cyber games with each other's critical infrastructure. As with the attack on Syria in 2007 the criticism of the *Stuxnet* operation was muted. Perhaps some thought it served some useful purpose in reducing some threat (e.g. to keep Iran from making the Bomb). What is little appreciated is that the majority of potential targets for *Stuxnet* type attacks are not in the Middle East but in the developed countries found in Europe, North America and parts of Asia that have critical infrastructures—potential targets that are far less protected (not located in underground facilities) and more vulnerable (more possibilities for penetration) to *Stuxnet* type attacks.

## 1.2. Saudi Aramco 2012

In December 2012 another nation's critical infrastructure was cyber attacked. Saudi oil company Saudi Aramco experienced a targeted cyber-attack on its computers. A cyber weapon called SCHAMOON succeeded in wiping clean over 30,000 computer hard drives. The attack seems to have been limited to the administrative part of the company and not the critical infrastructure parts involved with the production and processing of oil. However for the Saudis this cyber-attack was taken as an attack that threatened not just its critical energy infrastructure but its economy.[17] Although there was no conclusive proof it was strongly suspected that another Government's cyber power was responsible.[18] The message again was reinforced: cyber-attacks are an attractive and highly effective tool for inflicting damage on an adversary at low cost in terms of liability, preparation, delivery, and minimal

[17] AL Arabiya with AFP, „Saudi Aramco says cyber-attack targeted kingdom's economy“, *Al Arabiya News*, http://english.alarabiya.net/articles/2012/12/09/254162.html, 09 12 2012.

[18] Perlroth N., „In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back „“, *New York Times*, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html, 23 10 2012.

collateral damage. The problem was getting worse as there were indications that these attacks were counter strikes done in retaliation for earlier attacks.[19] In addition a pattern seemed to be emerging. Areas known to have long ongoing simmering conflicts like the Middle East were spilling into cyberspace as a new dimension of conflict and vice versa. One other example of this is the cyber-attack that took place against South Korean government news agencies and financial sites which resulted in over 30,000 computers and the data on them being destroyed.[20]

## 2. International Organizations' Reaction to the Actions of Their Members in Cyberspace

What was the reaction of the international community to these demonstrations of state sponsored cyber-attacks on another state's critical infrastructure? The answer: practically none. I remember attending meetings of the United Nations mandated Internet Governance Forum (IGF) in September 2010 which took place in Vilnius. Internet privacy and freedom of access were the dominating issues, yet as this author pointed out[21] the more serious national security question raising events in cyberspace that had a direct bearing on those issues were being ignored by the IGF. What was missing from the discussion in this and other international forums was what to do about the third source of cyber-threats – other states. The same states that are members of alliances and participate with others in conferences and forums discussing cyber security, internet freedom and defense policy.

However, attempts were made to address this issue of State involvement in cyber-attacks. The "Shanghai Cooperation Group" of nations (Russia, China, Tajikistan, Uzbekistan) did present a letter to the General Assembly of the United Nations in September of 2011 proposing an "International Code of Conduct for Information Security".[22] Among the proposals was one for states to refrain from using this technology against each other's critical infrastructure.

[19] Ibidem.

[20] Dunn J., „South Korean cyberattacks used hijacked patch management accounts", http://www.pcworld.com/article/2031860/south-korean-cyberattacks-used-hijacked-patch-management-accounts.html#tk.nl_today, *PC World*, 23 03 2013.

[21] Transcript, *Internet Governance Forum*, http://www.intgovforum.org/cms/component/content/article/102-transcripts2010/658-sop, 10 09 2010.

[22] Maurer T., „Cyber norm emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-security", *Belfer Center for Science and International Affairs*, http://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf, 09 2011, p.66-68.

However it was quickly dismissed by western nations[23] as too biased in favor of authoritarian states seeking to control on-line content and uncomfortable political activism. The West, however, is a bit two-faced here as they have long been showing signs of authoritarianism themselves. Witness the revelations of state domestic and foreign electronic spying in 2013 which supposedly took place even on the electronic communications of friendly states[24].

The OSCE has tried to tackle this issue. In 2011 during the Lithuanian Chairmanship of the OSCE a conference was held in Vienna that discussed whether the experience of the OSCE in arms control issues could be applied in cyber space. This author participated in discussions on possible Confidence and Security Building Measures (CSBM's) for cyberspace which took place in the summer and fall of 2011. An informal Work Group mandated by OSCE Decision PC1039 was tasked with coming up with draft CBM's which would be presented to the OSCE ministerial meetings later that year in Vilnius. While many proposals were discussed nothing that would in any way put limits or restraints on malicious State activities in cyberspace could be put on the table.[25] Alas, nothing could be agreed upon and no proposals for CBSM's were presented at the OSCE Ministerial.

The UN's International Telecommunications Union (ITU) organized the World Conference on International Telecommunications (WCIT) at the end of 2012 in Dubai. This was a most interesting conference in many ways. The ITU tried to foster some updates to the way world telecommunications was to be regulated. For example there were proposals to update the regulations to include something that was missing from the last time the regulations were approved in 1989: the Internet. While the WCIT meetings failed to reach an agreement on an updated set of telecommunications regulations to cover the Internet it illustrated another issue: the growing divide between East and West in regard to Internet Governance Issues. It was evident that there was a growing concern among non-Western nations in particular Russia and China over the West's domination (in particular by the United States) of the way the Internet was managed. Democracies tended to support a multi-stakeholder approach (minimal Government involvement) to Internet management while more authoritarian Governments sought more Government controls over content and use. While Internet freedom advocates were joyous over the failure of the

[23] Farnsworth T., „China and Russia Submit Cyber Proposal", *Arms Control Association*, http://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal, November 2011

[24] BBC, „Brazil and Mexico probe claims US spied on presidents", http://www.bbc.co.uk/news/world-latin-america-23938909, 2 09 2013

[25] I know this because I was one of those who attempted to make such a proposal., Author's note.

"UN to take over the Internet"[26] a dangerous split remained between East and West over the management of cyberspace.[27]

The *Tallinn Manual on the International Law Applicable to Cyber Warfare* is notable in regard to this East-West split. It was developed by an independent "international group of experts" at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence in Estonia.[28] The manual provides analysis and a guide on the applicability of established international norms on the new domain of cyberspace. Its views and findings are not binding but the list of "international" experts perhaps indicates how influential this Manual will be as a guide for future behavior in cyberspace. Its contributing experts come from the western democracies leaving out representatives of countries (especially from the East) that comprise the majority of Internet users. Leaving the East unrepresented among the list of contributors will do little to promote its general acceptance as a guide for policy makers seeking cooperation in solving issues of cyber security. It is hoped that in version 2.0 of the Manual a more representative list of world experts will be invited to participate.

## 3. How Have States Reacted to the Actions of Their Neighbors in Cyberspace?

As shown above the international community has not collectively made much concrete progress in addressing the malicious cyber activities of states in cyberspace. Cyberspace remains an ungovernable territory, like the "Wild West", but without any sheriffs or cavalry. States, however, have recognized this new danger and have responded by creating units specifically tasked with cyber defense. This is no small trend. In 2007 one study estimated there were over 120 countries with such units.[29]

Here is a short list of countries whose governments are known to have cyber defensive or offensive units: Australia, Belgium, Brazil, Canada, China, Finland, Germany, India, Iran, Israel, Japan, Malaysia S. Korea, N. Korea, U.K., U.S.A., and Russia. Probably the most publically known reaction to this

[26] Klimburg A., „The Internet Yalta", *Center for a New American Security,* http://www.cnas.org/theinternetyalta, 02 02 2013, p. 2.

[27] Gewirtz D., „Take action before the UN, Russia, and China hijack the Internet", *ZDNET*, http://www.zdnet.com/take-action-before-the-un-russia-and-china-hijack-the-internet7000008003/?s_cid=e539#postComment, 28 11 2012.

[28] NATO Cooperative Cyber Defence Centre of Excellence, http://www.ccdcoe.org/249.html, 2013.

[29] „In the Crossfire", *McAfee*, http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf, 2009.

activity has been the United States.[30] Cyberspace is a serious issue for the US as it continues to be a victim of cyber espionage and cyber-attacks. States have certainly taken notice that the US considers cyberspace to be an "operational domain",[31] is actively developing its Cyber Command, and is associated with the development and use of cyber weapons of the *Stuxnet* family and its suspected surveillance of domestic and foreign electronic communications.

China's military is associated with a cyber-warfare unit called PLA Unit 61398 which was recently exposed in a public report.[32] Information about Russian Government cyber units[33] have received less publicity but appear to be no less active than other cyber powers. Australia's Signals Directorate seems to want to let everyone know what it is up to. The motto on their website is "Reveal their secrets, protect our own" .[34] Nations are also actively working the market to obtain more information about preparing cyber-attacks and the weaponry to execute them with.[35] Of the highest value is information about unpublished software vulnerabilities known as "zero day". Knowledge of these vulnerabilities that can be exploited with a high probability of success can make a computer hacker rich and perhaps even land him a government job. What is the motivation behind these activities that have amounted to a "Cold War" like cyber-arms race among nations?

Perhaps they have understood the implications of *Stuxnet*. *Stuxnet* showed that malware can be designed as a cyber-weapon for targeting the critical infrastructure of a nation. The damage done can be real and, unlike a missile attack, it leaves little or no collateral damage and very little possibility to trace and determine the perpetrator's location. Using a cyber-weapon is cost effective. Yes, it is expensive, but cheaper than the cost of a jet fighter or bomber. The cost of developing, testing, and delivering *Stuxnet* for example may have cost about 10 million USD[36]. Not a bad price for disrupting the

[30] Sanger D., „Budget Documents Detail Extent of U.S. Cyberoperations", *New York Times*, http://www.nytimes.com/2013/09/01/world/americas/documents-detail-cyberoperations-by-us.html, 31 08 2013.

[31] U.S. Depatarment of Defense, *Department of Defense Strategy for Operating in Cyberspace*, http://www.defense.gov/news/d20110714cyber.pdf, p.5, 17 07 2011.

[32] Mandiant, *APT1 Exposing One of China's Cyber Espionage Units*, http://intelreport.mandiant.com/, 2013.

[33] Sridharan V., „Russia Setting up Cyber Warfare Unit Under Military", *International Business Times*, http://www.ibtimes.co.uk/articles/500220/20130820/russia-cyber-war-hack-moscow-military-snowden.htm, 20 08 2013.

[34] Australian Government, Department of Defence, http://www.dsd.gov.au/ 2013. (Website)

[35] Perlroth N., Sanger D., „Nations Buying as Hackers Sell Flaws in Computer Code", *New York Times*, http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html, 13 07 2013.

[36] Langner R., „The short path from cyber missiles to dirty digital bombs" , Langner Communications GmbH, http://www.langner.com/en/2010/12/26/the-short-path-from-cyber-missiles-to-dirty-digital-bombs/, 26 10 2010.

operations of a heavily fortified underground facility with no losses incurred on the part of the attacker and no blame incurred. The relatively cheap cost and the difficulty in attribution (identifying who is responsible for the attack) are the two main advantages for states seeking a more effective, safe, and deniable means for achieving a frustrated foreign policy objective. States may even feel driven to develop defensive/offensive cyber capabilities both to defend themselves against such attacks and also to deter them. Even though much has been written about *Stuxnet* since it first publically appeared in 2010 the international community has remained strangely silent. Nations are seeking to purchase information about "zero day" vulnerabilities with the intent of protecting themselves or for use in offensive operations of their own. However, this anxious activity, similar to drinking sea water when one is thirsty, can lead to the opposite result in terms of improving the climate of transparency and trust.

Some cyber powers like the US have tried to show some leadership in promoting common cyberspace policy. The US Government, for example, published its *International Strategy for Cyberspace* in May of 2011.[37] It proclaimed to the international community its goal: "to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace".[38] A noble statement by one of the world's leading cyber powers on common policy in cyberspace. However, this was presented two years after the release of *Stuxnet*—work widely attributed by many to the United States.[39] The issuing of this strategy while *Stuxnet* was appearing on many of the world's computers has made US cyber policy appear both malevolent and benign at the same time. One cannot blame other nations if they are confused. They must wonder whether the United States views cyberspace as an environment for cooperation or as a space for conflict.[40]

There is evidence that some states have not taken up the US proposal for peaceful use of cyberspace governed by respect for the rule of law. They

[37] The White House, *International Strategy for Cyberspace*, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, 05 2011.

[38] Ibid. p. 8.

[39] Sanger D., „Obama Order Sped Up Wave of Cyberattacks Against Iran", *New York Times*, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0, 01 06 2012.

[40] Healey J, *A Fierce Domain: Conflict in Cyberspace,1986 to 2012*, Cyber Conflict Studies Association, 2013, p.77.

instead have chosen to retaliate.  For example, after Iran's nuclear facility was cyber attacked with *Stuxnet* and after a cyber-attack against another part of its critical infrastructure (oil industry) occurred in April of 2012,[41] Saudi Arabia's oil industry was cyber-attacked in December of 2012.[42]  Serious cyber-attacks were directed at the US financial system in late 2012 and early 2013.[43] The United States was very quick to blame Iran for these attacks.[44] In light of these expanding and lasting attacks on energy and financial sectors one wonders whether this situation is perhaps getting out of hand.

## 4. Where Does This Lead and Why Should We Do Something About Securing Cyberspace?

Where does all this lead in terms of international peace and stability? The attractiveness of cyber weapons as a cheap, effective, deniable form of attack for the achievement of otherwise unachievable foreign policy objectives has not gone unnoticed by States. These weapons can be used to disrupt or destroy vulnerable information technology and telecommunications components. What we are talking about are the vulnerable strategic elements that form the backbone of national critical infrastructures responsible for electric power generation, telecommunications, financial systems, transportation and other structures whose processes provide services vital to the economy and social well-being of modern industrialized nations. The fact that attribution, meaning the identification of those responsible for the attack, is so difficult provides very tempting advantages for the attacker seeking an easy way for causing harm. However, it gives those concerned with defense a most uncomfortable sense of suspicion and uncertainty as to the intentions of their neighbors. Why is my neighbor spying on me?  Why are my neighbors creating cyber-commands? What do they plan to do (are doing) with them? Perhaps I need to create one to?  Satisfactory answers to these questions are difficult to find in this atmosphere of poor transparency and trust.  It is hard to disagree with

[41] Roberts P., „Iran Acknowledges Hack Of Oil Ministry", *Threat Post*, http://threatpost.com/iran-acknowledges-hack-oil-ministry-042312/76470, 23 04 2012.

[42] Al Arabiya and AFP, „Saudi Aramco says cyber attack targeted kingdom's economy" , *Al Arabiya* News, http://english.alarabiya.net/articles/2012/12/09/254162.html, 09 12 2012.

[43] Rothman P., „Cyber terror rages in the banking sector",  http://www.securityinfowatch.com/blog/10796084/cyber-terror-rages-in-the-banking-sector, 28 09 2012.

[44] Perlroth N., „In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back"  , New York Times, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html, 23 10 2012.

those who talk about the start of a cyber-arms race.[45]

One also has to consider the pressure leaders face in doing something when their nation's critical infrastructure is cyber attacked. It is quite possible that if retaliation is chosen it may be directed at an innocent country rather than at the true perpetrator. There is some evidence for example that the cyber-attack directed against South Korea in the spring of 2013 could have originated from either North Korea or China.[46] How can a country be sure that it has correctly identified the actual culprit behind the attack? This lack of certainty regarding attribution adds another element of instability in relations.

The use of cyberspace has been an issue of serious contention among major powers. The way that these powers have reacted in response has also increased the degree of instability in their relations with each other and with other nations caught "in the cross-fire". The accusations exchanged between the US and China over cyber espionage and cyber probing of each other's critical infrastructure offer good examples.[47] One writer, in discussing possible US motives behind *Stuxnet*, provided a chilling conclusion. He said that, in reacting to the attacks on its cyberspace assets, this cyber super power used *Stuxnet* to say to all potential adversaries: "Think twice before you attack us. This is a sample of what we can do. We will do it again".[48] One can perhaps understand the desire to deter a potential aggressor by bragging about one's own cyber weaponry, but for a cyberspace user living outside the United States it offers little comfort. It is incorrect to think that a cyber-weapon can be used to deter and influence others to change their behavior. In many ways this is a capability that is equally available to both powerful and less powerful states. Unlike the very high "membership requirements" of the nuclear club, any nation today can create or obtain from the market their own digital code for a cyber- weapon and become a cyber-power.

Another cause for concern comes from the degree of interconnectedness of systems. Cyberspace fundamentally supports the environment where modern commerce and international affairs take place. An angry nation or patriotic cyber army responding to a cyber-attack by directing its cyber weaponry at the supposed perpetrator country can have unpredictable consequences. This

[45] Guy-Philippe Goldstein , „How cyberattacks threaten real-world peace", Ted Conferences, http://www.ted.com/talks/guy_philippe_goldstein_how_cyberattacks_threaten_real_world_peace.html, 10 2011.

[46] Donohue B., „South Korea Blames North Korea for March Cyberattack", *Threat Post*, http://threatpost.com/south-korea-blames-north-korea-march-cyberattack-041013, 13 04 2013.

[47] Healey J., *A Fierce Domain: Conflict in Cyberspace, 1986-2012*, Cyber Conflicts Studies Association, 2013, p. 171-173.

[48] Morton C., „Stuxnet, Flame, and Duqu – the Olympic Games" in Healey J. ed., *A Fierce Domain: Conflict in Cyberspace, 1986-2012*, Cyber Conflicts Studies Association, 2013. p. 231.

is because cyberspace is so interconnected worldwide with other networks and systems. The attacks (and any counterattacks attempted by the target) will likely transit through an unpredictable number of networks and systems found in other countries. The cross border nature of critical infrastructure (electric grids or gas pipelines for example) make its also likely that such conflicts will have spill-over effects on other national infrastructures and institutions.[49] Retaliation for a cyber-attack by one nation whom it thinks is responsible, no matter how justifiable it may be, can have volatile consequences.

Even a case of cyber espionage can be interpreted as an act of war. (This was so for the U.S., when it attributed a cyber-espionage incident to Russia.[50]) Some may be quick to dismiss cyber espionage as part of an accepted "real world" practice. This is not quite the case when espionage is conducted electronically in cyberspace. Unlike traditional espionage, where a human steals information, cyber espionage activity is unique in the sense that when an electronic spy penetrates a system there is very little effort involved in changing from spy activities (downloading documents) to sabotage. A "spy" can leave behind a logic bomb in a critical system set to go off later on command. This is called "Preparation of the Battlefield". Once you have penetrated a system and established a presence there is very little difference between executing an act of espionage or sabotage. It is only a matter of pressing the ENTER key. This kind of preparation of the battlefield activity if detected by the victim can be very provocative and in the context of a crisis may easily escalate into serious conflict.

Another cause of tension among states is the use of cyber-attacks as an instrument to influence a neighbor's domestic politics[51]. This was a likely motive for the cyber-attacks on Estonia in 2007, for example. Patriotic cyber armies/militias that support their government policies or promote agendas of their own have become more active.[52] How will nations confront the consequences of these volunteer cyber militias in terms of their relations with other nations? How will they respond to other Governments complaints over attacks by these armies based in their territory?

[49] National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, http://www.nap.edu/openbook.php?record_id=12651&page=R1, The National Academies Press, 2009, p. 46-49.

[50] Elkus A., „Moonlight Maze" in Healey J. ed*., A Fierce Domain: Conflict in Cyberspace, 1986-2012*, Cyber Conflicts Studies Association, 2013., p. 152-160.

[51] Healey J., *A Fierce Domain: Conflict in Cyberspace, 1986-2012*, Cyber Conflicts Studies Association, 2013, p. 191

[52] McAfee Labs, *McAfee Threats Report: First Quarter 2013*, McAfee, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf, 2013, p. 33.

The bottom line is this: the advantages that cyber weapons provide for the potential attacker in terms of cost effectiveness and deniability are attractive and tempting, perhaps even too tempting not to use. Nations have recognized that they are increasingly dependent on cyberspace for their economic growth and well-being of their societies. In the absence of any "cyber police" to send for in times of need, nations are creating their own cyber capabilities. In this atmosphere of uncertainty and suspicion any cyber conflict can quickly lead to major conflicts among states. It is also likely that any traditional form of conflict between states will also be accompanied by a cyber-attack component which would add to the difficulty in resolving them. International organizations are the logical place to look for "referees" in this new and potentially deadly game.

## 5. What Can the International Community Do to Reduce the Danger of Escalating Conflict Resulting from the Malicious Activities of States In Cyberspace?

The task of proposing solutions regarding the malicious activities of states in cyberspace cannot be assigned to high technology specialists working in Ministry IT or Procurement departments, law enforcement agencies, secretive intelligence agencies, or by militarized cyber units. The complex issues involved in responding to and managing the effects of these activities that have an international dimension can only be solved by politicians and security policy makers. To be successful this work must be carried out in the context of a mobilized international community committed to developing internationally binding solutions. The goal would be an international agreement on norms of state behavior and a system for increasing trust, responsibility and transparency among states in in cyberspace.

## 6. Proposals for Addressing the Misbehaviour of States in Cyberspace:

*1. Commitment to restrain from malicious cyber activities directed against critical civilian infrastructure (financial, energy-utility, transportation and telecommunications).*

Rationale: The desire to protect national economies and civilians from financial loss or physical harm should be common to all nations. Certain state activities in cyberspace can be lead to misperception and instability in relations among states. For example, the placement of "logic bombs" or "back doors" in a nation's critical information infrastructure can be mistaken for "preparation of the battlefield" activity and could lead to rapid escalation of tensions. Cyber activities directed against the critical infrastructure of another state can also have significant cross-border and even regional effects due to the integration of financial systems, power grids, pipelines, and other modern critical infrastructure.

Something similar has already been mentioned in other proposals made by representatives of both East and West. One comes from the nation closely associated with Stuxnet. Richard Clarke, former adviser on national security for several U.S. presidents, has applied his extensive experience in nuclear arms control issues to the realm of cyberspace in his recent book, *Cyber War*. Read his proposal for a Cyber War Limitation Treaty.[53] Language prohibiting the use cyber weapons against critical infrastructure is also included in the Shanghai Cooperation Group proposals for an international code of conduct sent to the United Nations in 2011.[54]

Restraint is not enough of a pledge; it also requires an acceptance of responsibility for meeting one's obligations which leads to proposal 2.

*2. Commitment on national cyberspace liability. States agree to accept responsibility for malicious cyber activities taking place within their cyberspace jurisdictions or transiting through them.*

Rationale: Nations need to agree on minimum obligations for securing their national cyberspace. Emphasis should be placed on the state's obligations to react to incidents originating from or transiting through their cyberspace jurisdictions. Nations should insure for example that national internet service providers (ISP's) and law enforcement agencies take appropriate steps toward individuals, groups and/or information and communication technology equipment found to be participating in a cyber-attack. This also implies that states agree to develop a capacity for dealing with cyber security matters. This means establishing appropriate laws and structures (national CERTs, law enforcement entities etc.) needed to implement the commitment.

This is also not a new idea. Scholars in the United States have been

[53] Clarke R., *Cyber War: The Next Threat to National Security and What to do about it,* Harper Collins, 2010. p. 268-271.

[54] Ministry of Foreign Affairs of the People's Republic of China, „China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations", *Ministry of Foreign Affairs of the People's Republic of China,* http://www.fmprc.gov.cn/eng/wjdt/wshd/t858978.htm, 13 09 2011.

discussing the merits of states accepting responsibility for what goes on in their cyber jurisdictions. Examples of this policy thinking include Chris C. Demchak's and Peter Dombrowski's paper covering cyber borders and jurisdictions. They argue that cyberspace is no longer a public commons or prairie where all can roam and do as they wish. There is so much development and interest at stake for a nation's security that the establishment and control of "cyber borders" is an important step toward insuring protection of their critical infrastructure from cyber based threats.[55]

Related to responsibility and liability is the problem of attribution. The level of difficulty in carrying out cyber-attacks and probability of getting caught must be raised higher. The establishment and control by a state of its cyber borders will make it more difficult for cyber-attacks to go by unnoticed. However, the unsuccessful effort up till now of placing the blame needs to be shifted from trying to identify who is actually attacking to identifying "what nation, if any, is responsible".[56] It is the State that should be held responsible for insuring the control of its cyber borders and for making sure that malicious cyber activity originating or transiting through its cyber jurisdiction is monitored and controlled. The full burden of responsibility for reacting to and investigating an attack should not be placed on the victim but on those closest to and capable to react to the incident;

*3. Monitoring of implementation of agreed upon commitments listed above. States agree to create a coalition of willing experts and institutions to monitor and advise on violations of the above two agreements.*

Rationale: Some means must be available to monitor and inform participating states of malicious cyber activities taking place or transiting through their cyber jurisdictions. An institution consisting of experts that can monitor and provide objective evaluation of violations to commitments should be established. This will provide for a capability to apply "soft pressure" on nations that are slow or reluctant to act on reported malicious activity taking place in their cyber jurisdictions.

Again this is nothing that should be new to anyone working in international relations. This is not naive idealism. In questions where the need is recognized and where it really matters states have banded together and signed international agreements and conventions. This has been especially so with prohibiting the use of weapons of mass destruction. One possible model

[55] Demchak C., Dombrowski P., „Rise of a Cybered Westphalian Age", *Strategic Studies Quarterly,* 5 (1), p. 54-57, http://www.au.af.mil/au/ssq/2011/spring/spring11.pdf, 2011.

[56] Healey J., ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Studies Conflict Association, 2013, p. 265.

for dealing with the production and use of cyber weapons by states is the International Convention on Chemical Weapons. Still perhaps remembering their use in World War I and in recognition of the advances in technology that could facilitate the use of chemical weapons and amplify their potential for harm, a convention entered into force in 1997. Over 190 nations have signed it, representing 98% of the world's population. Associated with the agreement, the Organization for the Prohibition of Chemical Weapons (OPCW) was created to monitor and follow up implementation of the convention.[57] The Convention on chemical weapons can serve as a useful model when considering implementation of the 3 above mentioned proposals. The work of the OPCW at the time of this writing has made an active contribution to resolving the crisis in Syria. The merit of this work was recognized internationally in 2013 when the OPCE was awarded the Nobel Peace Prize.

The Asia Pacific Computer Emergency Response Team coalition (APCERT) offers an example of regional cooperation. APCERT is made up of CERTS and Internet Service Providers of Japan, China, and South Korea. APCERT treats "the Internet and its health as a connected common shared infrastructure".[58] The coalition has been successful at addressing cyber incidents arising from political conflicts amongst its members.[59]

One example of an ad hoc yet effective global response to a perceived common threat in cyberspace is the work of the CONFICKER work group in 2008-2009. Governments for the most part failed to recognize the growing danger to the Internet from the creator of CONFICKER worm and the growing number of infected computers that could be commanded to action at any time. The fight to save the Internet from this new and potentially destructive worm was taken up by a group of volunteers that included gifted private individuals, Internet service entrepreneurs, and non-government organizations. This core group of individuals was able to muster enough cooperation worldwide to analyze, monitor, and defuse the Internet bomb that was CONFICKER.[60] These are just a few examples of what a motivated international community can do.

[57] Organisation for the Prohibition of Chemical Weapons, http://www.opcw.org/chemical-weapons-convention/

[58] Ito Y., „Making the Internet Clean, Safe and Reliable Asia Pacific Regional Collaboration Activities", *The Institute of Electrical and Electronics Engineer*s, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5978796, 2011.

[59] Ibidem.

[60] Bowden M., *Worm: The First Digital War*, Atlantic Monthly Press, 2011 p. 221.

## Conclusion

Cyberspace, which is more than the public internet, can no longer be understood simply as a global commons for conducting one's business, visiting web sites and reading emails. It must be considered a domain critical to a nation's wealth and its citizens' well-being—a fact that would become painfully obvious the minute one of these fragile processes or services is interrupted for more than a few hours. This space holds things of great value that are now vulnerable and must be protected. The recently publicized arrests of cyber criminals and hacktivists, although very welcome in that they provide good examples of cooperation and increasing effectiveness of law enforcement, represent only a partial success at insuring a safe cyberspace. The costs of cybercrime do not represent the true scale of the danger. In fact, the costs in terms of the world economy could as one study conjectured amount to nothing more than the value of a rounding error in a 14 trillion a year economy.[61] Nor is an emphasis on securing information and information systems (misleadingly called "critical information infrastructure") enough to insure the safety of critical infrastructure from cyber-attack. The real danger to be considered in securing cyberspace is the unregulated malicious activities of states in cyberspace—especially those activities directed at paralyzing the control systems and operations of electric grids, gas pipelines, transportation systems and other utilities so fundamental to the life of modern civilization. While cyberspace is governed by the laws of physics and continues to be maintained by highly skilled technologists, they alone cannot solve this problem. Nor can cyberspace weapons technology be used to solve current conflicts in the world. It has been recently proposed that a humanitarian demonstration of cyber weapons be used in the current Syrian conflict.[62] This brings to mind some of the deliberations of 1945 over first use of the Atomic Bomb – a demonstration as warning. One strongly doubts whether complex conflicts such as in the Middle East can be solved by pressing the ENTER key. If such proposals are being openly discussed, then things are getting out of hand.

The international community must strive for a deeper understanding of the nature and importance of cyberspace. Needed are new cyber diplomats and cyber politicians that share a common knowledge of what is at stake and share

[61] Center for Strategic and International Studies, McAfee., „The Economic Impact of Cybercrime and Cyber Espionage", McAfee Inc. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf, July 2013, p.3.

[62] Healey J., "Why the U.S. Should Use Cyber Weapons Against Syria", *Defence One*, http://www.defenseone.com/technology/2013/08/why-us-should-use-cyber-weapons-against-syria/69776/, 31 08 2013

an understanding of the danger. There are signs that cyber politics is starting to be recognized as a new security policy field.[63] State cyberspace activities are best understood as international security issue not as an information security issue.

This problem cannot be handed off to law enforcement, militaries, or intelligence agencies to solve. There is a tendency for these bodies to work in secrecy. Cooperation among a wide range of public and private sectors is a key factor in making cyberspace safe. Secrecy, however, will make cooperation more difficult. This question must be addressed by the civilian leadership in governments in a transparent way for only they can manage the full aspects of national and international security.

2014 will mark 100 years since the start of World War I. Historians continue to comment and scratch their heads over why such a destructive and tragic war had to happen. One of the big surprises of WWI was the application of new technologies for lethal effect in terms of millions of lives lost from the machine gun, mustard gas, aerial bombing and torpedoes. Perhaps in the effort to address the dynamic challenges presented in this article regarding state behavior in cyberspace we can use a lesson from that war? The American historian, Barbara Tuchman, in her book *The Guns of August* about the start of the First World War, perhaps said it best when she wrote: “One constant among the elements of 1914 – as of any era – was the disposition of everyone on all sides not to prepare for the harder alternative, not to act upon what they suspected to be true.”[64] Perhaps the nations that participated in that war will consider this and act to insure that cyber weapons technology will not be the cause of similar tragedies in the twenty-first century?

*October 2013*

[63] Choucri N., *Cyberpolitics in International Relations*, The MIT Press, 2012, p.238.

[64] Barbara Tuchman, *The Guns of August*, Macmillan, New York: Ballantine Books, 1962. p. 84.