Cyber Security and the Need for International Governance

Monday, May 16, 2016
Law Student Writing Competition Winner

Cybercrime is a borderless crime where the repercussions and consequences are endless; the United Nations’ Security Council should have a prominent role in establishing international laws to govern and mitigate the effects of these cybercrimes that plague a multitude of nation States. At the end of World War II, there was a need to organize the Security Council to maintain international peace. However, the chief concern in 1945 was to have an armed troop ready to prevent invasions by one country to another. But with the advances in technology and the invention and widespread use of the Internet, a new threat emerged against all nation States—one that cannot be fought by troops on the ground. The Security Council is the authorized agency to implement an international policy for cyber-security to combat the threats from cyber-warfare, cyber-terrorism, and other cyber-acts.

In part I, I explain the inception of the Security Council and describe its purpose from the date of inception in 1945 to current times as it relates to cyber security. In part II, I define cyber security and the emerging trends of cyber-security. Finally, in part III, I describe the Security Council’s efforts to implement an international policy that enforces cyber-security.

I. The Security Council

In 1945, the Security Council was set up as a part of the United Nations with the primary responsibility of maintaining international peace and security. The Security Council is responsible for formulating, with the assistance of the Military Staff Committee[1], plans to be submitted to the Members of the United Nations for the establishment of a system for the regulation of armaments. The Security Council may investigate any dispute, or any situation which might lead to international friction or give rise to a dispute, in order to determine whether the continuance of the dispute or situation is likely to endanger the maintenance of international peace and security. The Security Council determines the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decides what measures should be taken in accordance with Articles 41[2] and 42[3], to maintain or restore international peace and security.

Article 41 gives the Security Council the autonomy to decide what measures not involving the use of armed forces are to be employed to give effect to its decisions[4]. The decisions under this article may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations. Article 42 provides that if measures in Article 41 prove ineffective, then the Security Council can consider additional measures that include armed forces in order to maintain or restore international peace and security.[5] All functions of the United Nations relating to strategic areas shall be exercised by the Security Council.
In 1945, when the Security Council was established its role was based on member States coming together for the maintenance of international peace and security with a standing army to act as the global police. However, present day, one of the biggest threats to international peace and security is not necessarily a physical invasion that can be prevented or mitigated by ground troops. With the advances in technology and the advent of the Internet, member States must now be concerned with cyber activity and cyber warfare. The Internet is borderless unless specific interventions are taken to alter this state of nature. An Internet user can take actions in one country that will have outcomes in another country without the user ever leaving their own country. Therefore, there is a growing and perhaps imminent need for States to have international cooperation in handling cyber security; and, according to Article 25 of the UN Charter, the Security Council is the only legitimized authority to create binding international law: “The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter.”

One of the reasons the Security Council has struggled to create a comprehensive plan is because the member States have not been able to agree upon common terms and definitions about what cyber-warfare and cyber-attacks really are. For example, authoritative nation States like China and Russia view it as Information Security because those countries are more concerned about the content that is breached. Whereas the United States and its Western partners look at it as Cyber Security because they are more concerned about the process by which the attack occurs due in large part to their views on freedom of speech. Another reason the Security Council has struggled to create a comprehensive plan is due to the fact that the member States have been slow to realize an international plan is necessary and now even critical for the maintenance and sustainability of international peace. For example, 1998 was the first year that the Russian government introduced a resolution in the First Committee. The 1998 draft resolution was adopted as Resolution 53/70 on January 4, 1999. The key elements of this resolution for an “international computer security treaty” include:

- The military potential of information and communication technology for the first time as well as an expression of concern about the use of such technology “inconsistent with the objectives of maintaining international stability and security” which was Russia’s position.
- The need to prevent cyber-crime and cyber-terrorism which was the US’s position.
- And, to invite member states to inform the Secretary-General notably on their view regarding “definitions” and the development of “international principles”.

The resolution was adopted by the General Assembly without a vote, but the push for an international treaty was met with skepticism by the US and European states. They were suspicious that a treaty of this sort could be used to limit the freedom of information under the guise of increasing information and telecommunications security. Therefore, an international treaty was not made.

However, the UN has not overlooked the growing need around cyber-security. The International Telecommunication Union (ITU) is the UN’s organization that has most responsibility for practical areas of cyber-security. It is a treaty organization and is the only UN organization working on cyber issues with the status of treaty organization. The ITU, a Specialized Agency under article 57 of the UN Charter, plays an important role in setting technical standards. In its efforts to support a cyber-space initiative, the ITU considers cybercrime as one of its top three priorities.

II. Cyber Security

Definitions

Cyber is a prefix that refers to electronic and computer based technology. Cyber-space is “an operational domain framed by use of electronics to...exploit information via interconnected systems and their associated infrastructure.” Cyber-space is a “unique hybrid regime of physical and virtual properties, hardware and software, which is all computer networks in the world including the Internet as well as other networks separate from and not linked to the Internet.”

Cyber security, information and telecommunications technology in the context of international security, was a term first introduced by the Russian Federation in 1998. As defined by the ITU, cyber-security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.

Cyber-security threats exist for three reasons: 1) flaws in the design of the Internet, 2) flaws in the hardware and software, and 3) the move to put more and more critical systems online. Further, there are four areas of cyber security: 1) Espionage, 2) Crime, 3) Cyber war, and 4) Cyber terrorism. These four areas of cyber security can...
further be categorized into two streams – cyber warfare and cyber-crime. Cyber warfare is the unauthorized penetration by, on behalf of, or in support of, a government into another nation’s computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, or falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer system controls. It is a politico-military stream that is concerned about how information technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States. Alternatively, cyber-crime is an economic stream focused on the criminal misuse of information technologies.

Emerging trends - cyber threats

There has been an emergence in cyber-crime since the exponential rise in the Internet in 1998. Prior to 2000, a cyber-intifada between Israeli and Palestinian hackers led to an increase in violence at the outset of the second intifada in 2000. The dispute between India and Pakistan over Kashmir, had an ongoing cyber element involving groups of both sides of alleged State sponsorship. By 2007, for the first time cyber-warfare made major headlines. “By some counts, more than six countries experienced cyber assaults between 2007 and 2010, and at least 34 private companies were attacked in the early months of 2010 alone.” Cyber security was making front page headlines in 2010.

In 2015, cybercrime was viewed as a service. People can go to the dark web and hire a hacker. Mobile technology provides for a larger scale attack because there are more users of mobile technology than computers. A large scale breach is much more common because it’s more profitable. Small to medium-size enterprises are targeted because they have limited resources to invest in protection.

III. The Security Council’s Efforts to Enforce Cyber Security

Cyber threats

Existing and potential threats in the realm of information security are among the most serious challenges of the 21st century. They identify criminals, terrorists, and states as potential perpetrators. Individuals, businesses, national infrastructures, and governments are identified as potential victims. The threat is considered to be large enough to pose a risk to “international peace and national security” as states are found to develop cyber warfare capabilities.

Some of today’s current cyber threats come from China. China is aggressive in its cyber intrusions and cyber theft of intellectual property. China’s cyber operations have been so frequent and serious that they have been the subject of repeated diplomatic, even presidential, entreaties and complaints.

In March 2011, a cyber-attack of a foreign intelligence service hacked the computer system of RSA Security, a major civilian information security company, and gained data pertaining to the manufacture and capabilities of the tokens that RSA Security supplies to the Pentagon. RSA has tens of millions of dollars’ worth of contracts across the federal government. Agencies with large contracts included the Department of Defense and its service branches. Rather than attacking the Department of Defense directly, the cyber-attack targeted the firm that provided cyber security for the computers. Three months later it was confirmed that the hackers used stolen RSA token data and attacked Lockheed Martin, one of the nation’s largest defense contractors and makers of fighter aircraft and satellites.

In September 2007, seventy-five miles inside Syria, at least four Israeli F-15 Eagle and F-16 Falcon fighter-bombers attacked and destroyed their Syrian target. Israeli warplanes managed to penetrate Syrian airspace, conduct an attack, and escape, all without a shot fired at them by Syria’s modern air defense system. “Israel screened its kinetic attack with a cyber-attack that cloaked Syrian air defense radar screens with a false image of a clear sky,” says Richard Clarke, former U.S. National Coordinator for Security, Infrastructure Protection, and Counterterrorism.

In May 2014, the U.S. indicted five Chinese military officers for cyberespionage. In May 2015, six Chinese men were indicted in code theft from U.S. tech companies under the Espionage Act. Two of the individuals worked for U.S. companies. One of the individuals was a Chinese professor. In 2015, the Japanese equivalent of the Social Security Administration lost 1.5 million records in a cyber-attack.

Current efforts to enforce cyber security

Given the increased frequency in cyber-attacks transnationally, many nations joined in to come up with an
international treaty to implement cyber security initiatives. The Washington Post wrote in its article titled “15 nations agree to start working together to reduce cyber-warfare threat” that “A group of nations – including the United States, China and Russia – for the first time signaled a willingness to engage in reducing the threat of attacks on each other’s computer networks”. Pointing out that “The Russians proposed a treaty in 1998 that would have banned the use of cyberspace for military purposes”, the journalist quotes Robert Knake as considering the new development as being “part of the Obama administration's strategy of diplomatic engagement” because in the words of an Obama administration official “There’s been an increased understanding of the international need to address the risk.”[29] Since the start of his administration, President Obama has issued three executive orders to address cybersecurity:

1. Executive Order 13636 (February 2013) to improve the critical infrastructure for cybersecurity.[30]
2. Executive Order 13691 (February 2015) to promote the sharing of information amongst the private sector to provide greater cybersecurity.[31]
3. Executive Order 13694 (April 2015) to allow the government to confiscate the property and money through the banking system of those engaged in malicious cyber-enabled activities.[32]

However, these are domestic policies that have been put into place. The legitimacy of creating an international policy for combating cyber security flows from the Security Council’s primary responsibility for the maintenance of peace and security, which may be carried out by means of the mandate in the UN Charter. Member states of the UN help to create international law that applies to cyberspace, but the international law only applies at the state level and not the individual level which means member states must comply but it is left to the member states to enforce the international laws upon its citizens.[33] However, there are challenges to having an international policy and law on cyber security. Challenges to the Security Council combatting cyber terrorism and enforcing cyber security exist in many areas. One of the challenges with the Security Council is being able to utilize cyber operations to neutralize networks as part of a tool for peace. The SC has not been able to reach a consensus as to whether this act would amount to an attack under the laws of armed conflict. Part of the debate is due to the fact that the network is neutralized rather than destroyed. Member states agree that destruction of a network would fall under the laws of armed conflict, however, neutralization of a network enables the country affected to have its network restored once the conflict ends. Since the network is restored does this action really constitute an armed conflict or unarmed conflict? The SC members have not been able to agree. Peace operation mandates in Security Council resolutions almost always call on member States to provide assistance to peace operations.[34] In some cases they require States to ensure that their nationals, individuals, and firms within their territory or subject to their jurisdiction refrain from particular behaviors.[35] Before States will provide their cooperation, they will have to agree on the international policy.

Another challenge with the Security Council having the power to regulate cyber operations in various countries involves an infringement on individual rights such as the freedom of speech. Online content such as extremist websites, highly offensive video footage, and social media, have the potential to inflame, exacerbate and ignite tensions on the ground in areas where the peace operations are working. If online content has the ability to incite riots, then the removal or blockage of this content has the ability to promote peace or at the very least not interfere with peace efforts. For example, during the Arab Spring, the Egyptian government shut off access to the Internet for four days. India blocked access to approximately 250 websites in an effort to stop the spread of videos and images that caused the Bangalore panic. Other countries such as China and regimes in the Middle East and North Africa engage in heavy web filtering and censorship.[36] The Afghan government pushed Internet providers in that country to bar access to websites hosting an anti-Islamic video in order to head potentially violent demonstrations.[37]

In a “Joint Declaration on Freedom of Expression and the Internet,” rapporteurs on freedom of expression from the United Nations, Organization of American States and the African Commission on Human and People’s Rights and the Organization for Security and Cooperation in Europe’s representative on freedom from the media stated, “cutting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds.”[38] However, even though freedom of speech should be recognized and not constrained, there are limitations that should exist in special circumstances such as when the content amounts to incitement to commit crimes, such as genocide or certain other forms of hate speech. Blocking the Internet or certain parts of it should be justifiable and legal for the sake of peace operations regulated by an international policy created by the Security Council.

Despite the challenges and opposition to the development of an international policy that member States can agree on, they do agree on the fact that the policy is needed. The benefits of this policy far outweigh any individual rights that might be maintained by individual member States. The SC must continue to forge ahead to define terms that member States can agree upon and implement an international policy that will provide cyber-
Conclusion

Moving forward it is expected that many international conflicts will contain a cyber-element. To date there is no public record of cyber operations being used by a UN peace operation. However, there is a need for governance of cyber operations to enforce cyber security because there needs to be a way for countries to work together in an agreed upon manner to deal with cyber threats that may destabilize peace operations. Although the five Chinese hackers were indicted in May 2014, “it falls short of a credible response that may actually change China’s behavior because the Department of Justice’s (DOJ) indictment is not a credible deterrent.”[39] There’s no possibility of extradition, and no further cost imposed on the Chinese economy by the U.S. Government short of imposing economic sanctions.[40]

The Security Council should maintain international peace in the cyber context. Moreover, the suggestion that the United Nations should employ specific personnel to deal with the increasing number of cyber incidents taking place between States is indicative of the relevance of cyber operations for the conduct of UN-mandated peace operations.[41] Initially the Security Council was organized to enforce operations in ongoing conflicts, but the thought was that these conflicts would involve operations where troops on the ground would be needed. However, with the advances in technology and the emergence of the Internet, the role of the Security Council must change to deal with the ongoing and growing number of cyber-attacks.

When a cyber-operation directed against a peace operation is severe enough to amount to armed force, meaning the operation caused death or injury to a person, or physical damage, then the UN forces are authorized to use force in self-defense. But, the challenge is whether the UN in its peace enforcement operation, has authorization under Chapter VII to use force against cyber threats that do not amount to a use of force. Under Article 41 of the Charter, the Security Council may mandate a non-forceful measure to be taken in situations it deems to be a threat to the peace, breach of the peace or act of aggression. Regulating cyber activity, combatting cyber terrorism, and providing cyber security should all fall under this article.

Specifically within the US, cyber security is the third priority for FBI initiatives falling behind terrorism and counter-intelligence; however, the FBI anticipates cyber security being the number one priority in the next couple of years. Corporations and law firms are at risk as well. Corporations and law firms maintain trade secrets, personal data, patents, customer information, etc. and most still do not have cyber security policies in place. A lot of the different industries are now being regulated by federal agencies that are creating regulations around cyber security. No country, no industry, no organization, and no corporation are exempt from the threat of a cyber-attacks, cyber-warfare, and cyber-threats. The consequences of a cyber-attack is bottomless – they range from economic devastation ($67 million) as seen with massive data breaches within companies like Target[42] and The Home Depot where its estimated that the cost is upwards of $197 per person with 57 million records compromised[43], to nuclear meltdowns with the Stuxnet virus against Iran where the virus went undetected for over a year.[44] These cyber-attacks, and others like them, further substantiate the need for the UN’s Security Council’s need to regulate and mandate international laws designed to govern the growing number of international cyber-attacks that are both borderless and bottomless.

Works Cited

Lotrionte, Catherine. Symposium: International Law and the Internet: Adapting Legal Frameworks in Response to Online Warfare and Revolutions Fueled by Social Media: State Sovereignty and Self-Defense in Cyberspace; A Normative Framework for Balancing Legal Rights, 26 Emory Int’l. Rev. 825


National Security Institute: Latest Developments in International Cyber Security
https://connect.excelsior.edu/p2rltoxx6nc/?launcher=false&fcsContent=true&pbMode=normal


Solis, Gary D. Cyber Warfare, 219 Mil. L. Rev. 1


[2] Id.

[3] Id.

[4] Id.

[5] Id.

[6] Id.


[8] Id.


[13] For an overview of the International Relations literature and cyber security, see Eriksson et al; Nazli


[15] Nye, 2010:3; Clarke and Knake, 2010: 70

[16] Nye, 2010:3; Clarke and Knake, 2010: 73


[18] UN General Assembly A/RES/53/70

[19] UN General Assembly A/RES/55/63

[21] National Institute for Cybersecurity: https://connect.excelsior.edu/p2rltoxx6nc/?launcher=false&fcsContent=true&pbMode=normal

[22] Id.

[23] Id.

[24] Id.

[25] Id.

[26] Li Zhang, A Chinese Perspective on Cyber War, 94/886 INT’L REV. RED CROSS 801 (Summer 2012) (offering a different, far milder viewpoint)


[29] Nakashima, 2010


[33]https://connect.excelsior.edu/p2rltoxx6nc/?launcher=false&fcsContent=true&pbMode=normal


