CHATHAM HOUSE

Chatham House, 10 St James's Square, London SW1Y 4LE
T: +44 (0)20 7957 5700 E: contact@chathamhouse.org
F: +44 (0)20 7957 5710 www.chathamhouse.org
Charity Registration Number: 208223

International Law: Meeting Summary

Cyber Security and International Law

Mary Ellen O'Connell

University of Notre Dame Law School, US

Louise Arimatsu

Chatham House

Chair:

Elizabeth Wilmshurst

Chatham House

29 May 2012

INTRODUCTION

The 2011 US International Strategy for Cyberspace states that the US reserves 'the right to use all necessary means - diplomatic, informational, military, and economic - as appropriate and consistent with international law' to respond to concerns of all types in cyberspace. The meeting focussed on what international law permits in terms of response to these concerns, emphasizing that the right to use military force is limited in international law.

The participants included practising lawyers, academics and representatives of government, business, and NGOs.

Mary Ellen O'Connell

'Cyber Mania'

Cyber security is considered to be a hot topic in international law today and very pertinent to international security discussions. It is crucially important that civil society have access to safe and secure internet.

US General Dempsey believes that the US is more vulnerable than previously in terms of security and one chief cause, according to him, is the prospect of cyber-attacks. Others are in agreement with this point of view and even believe the US and other nations are fighting a cyber-war today.

This perspective is referred to by some as 'cyber mania' and is regarded as an overreaction to the threat of cyber-attacks. The major challenge to governments is to ensure that people are primarily protected from crime and espionage on the internet. The vast majority of cyber-attacks are not carried out by government-sponsored hackers but by criminals intending to steal business secrets and financial information. Therefore, there have been strong attempts to discourage governments characterising the internet as being seen a war-fighting problem.

Singer and Schachtman argue that analogies to war fighting, especially fighting the Cold War, are detrimental to preventing the real challenges to cyber security, crime and espionage. We can already see the negative consequences of analogising such incidents to war in gaining greater cyber security. Singer, Schachtman, Mueller and others are arguing that this approach is fundamentally flawed if the goal is secure and accessible internet.

To fit the internet security problem into the war-fighting category has also led to flawed analysis of the relevant international law. There is appropriate international law relevant to supporting commerce and communication on the internet, but that law is not the law of international armed conflict.

How are we inventing a cyber war problem?

Internet security concerns are as old as the internet itself. There was an attack in 1998 by some 3000 Chinese hackers on Indonesian government sites. Since then, there have been tens of thousands of attempts to hack into major computer networks belonging to defence ministries, banks and the media. Such incidents are happening daily. Most of these cyber intrusions have espionage or theft as the purpose and are typically categorized as 'computer network exploitation' (CNE). A smaller group is being referred to as 'computer network attacks' (CNA). Perhaps these should better be referred to as 'computer network interference' (CNI), as opposed to CNE or CNA. CNI would be closer to the language of economic or trade injury than 'attack', which is a term more closely associated with the military category.

There are three cases that are constantly discussed to support the view that internet security belongs primarily to military security. These are the following:

1) **Estonia & NATO, April 2007**: In response to the moving of a Soviet War Memorial, hackers began interfering with Estonian government websites through distributed denial of service attacks. Hackers defaced certain sites and redirected users to images of Soviet soldiers. This interference lasted approximately about a month, affecting several banks and newspapers. Estonian officials claimed it was the same as if a conventional military force had closed down Estonia's ports and referred to the episode as 'cyber-war'. The origin of the cyber-interference remains uncertain today. It was widely believed to have been instigated by Russia but experts were never able to establish this. Some argued that Estonia was attacked in a way that triggered

the North Atlantic Treaty's (NATO) Article 5. NATO did not respond with a counter-attack, but it did establish an internet defence facility in Estonia, called the Cooperative Cyber Defense Center of Excellence (CCDCOE). Estonia itself has now created a volunteer unit of cyber-experts akin to the US National Guard and has become a leader in determining ways to defeat online interference.

2) **Georgia-Russia, 2008:** This was the first known use of the internet during a conventional armed conflict to interfere with civilian use of the internet; it occurred in the 2008 conflict in the Georgian enclave of South Ossetia. Georgia triggered the conflict by attacking Russian soldiers who were part of a peacekeeping contingent in South Ossetia under the terms of a Georgia-Russia treaty of 1991. On the night of 7-8 August, Georgia staged a conventional military attack, killing approximately a dozen Russian soldiers and wounding many others. Russia conventionally counter-attacked pushing to within 35 miles of the Georgian capital, Tbilisi. Georgia claimed that Russia initiated distributed denial of service (DDoS) attacks against a number of Georgian websites, including government sites, media sites, and commercial sites. The interference last approximately a month. The physical fighting had lasted about a week.

3) **Stuxnet, 2009-2010:** A computer worm, dubbed Stuxnet, infected computers manufactured by Siemens and used in the Iranian nuclear programme. The worm is believed by experts to have been created by the United States military with assistance from Israel and scientists at Siemens. The effect of the worm in Iran was to cause centrifuges to turn far more rapidly than appropriate. In early 2011, officials in Israel and the US announced that Iran's nuclear programmes had been set back by 'several years.' The Stuxnet worm, however, affected computers in other countries as well, including India, Indonesia, and Russia. It is believed that 40 per cent of the computers affected were outside Iran. Stuxnet is said to be the 'first-known worm designed to target real-world infrastructure such as power stations, water plants and industrial units.'[1] Ralph Langner, a German computer security expert, was thought to be convinced that Stuxnet is a government produced worm: 'This is not some hacker sitting in the basement of his parents' house. To me, it seems that the resources needed to stage this attack point to a nation state.'[2]

In the US, the Department of Defense (DOD) is steadily taking the lead. In 2010, the Pentagon established Cyber Command. It is a subunit of Strategic Command, one of the nine combatant commands of the US's Unified Command System.

Cyber Command has been given a wide mandate. It not only has responsibility for defending DOD information networks, it must 'prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.'[3]

Singer and Schachtman believe that DOD's new cyber strategy is based on conceiving of cyber security in a way similar to the US's Cold War strategy. They relate that the classified version of the cyber strategy presents;

---

[1] Jonathan Fildes, "Stuxnet worm 'targeted high-value Iranian assets', 23 September 2010, cited at: http://www.bbc.co.uk/news/technology-11388018

[2] *Ibid*.

[3] US Department of Defense, Cyber Command Fact Sheet, May 25 , 2010, cited at: http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf

> 'a new doctrine of 'equivalence', arguing that harmful action within the cyber domain can be met with parallel response in another domain. Swap in the 'conventional' and 'nuclear' for 'cyber' and 'kinetic' and the new doctrine is actually revealed to essentially be the old 1960s deterrence doctrine of 'flexible response', where a conventional attack might be met with either a conventional and/or nuclear response. The Pentagon's Cyber Command and Beijing's People's Liberation Army's Third Army Department now fill in for the old Strategic Air Command and the Red Army's Strategic Rocket Forces.'[4]

In another related development within the US, in 2011-12, Congress began considering new legislation on cyber security. One group in Congress prefers to keep the primary authority for cyber security in the Department of Homeland Security (DHS), but another group is adamant that the Pentagon take the lead. Senator John McCain is one who objects to giving DHS more authority, preferring the emphasis to be with Cyber Command and the National Security Agency (NSA). McCain has argued against turning DHS into a 'super regulator'. General Keith Alexander shares McCain's concern. Alexander is, currently, both the head of the Cyber Command and the Director of the NSA. McCain and Alexander point out that Cyber Command and the NSA already have greater technical expertise than DHS, and use this as an argument to continue to favour the military over DHS with resources and legal authority.

Plainly, some of the pressure to militarize cyber security is being driven by business concerns in the military security sector. From that perspective, consultant Mike McConnell wants to push the idea of thinking about cyber security in terms of Cold War deterrence. He stresses the need for a strategy of both deterrence and pre-emption, depending on the nature of the threat.

The Law Restricting Cyber war

As already indicated at the outset, the emphasis on cyber space as 'battle space' is in tension with the international law governing the use of force. Some prefer to dismiss international law from the discussion altogether. Others do not exclude international law but interpret it in ways that in effect exclude it. In May 2011, President Obama indicated that international law would play a role in US cyber security planning, but he also indicated that it would be international law as interpreted by those who advocate a broad right of the United States to resort to force. This is seen in the *International Strategy for Cyber Space*; the White House announced:

> When warranted, the United Sates will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an *inherent right to self-defense,* and we recognise that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military partners.[5]

This signals a reading of the United Nations Charter (UN Charter) which sidesteps the express term 'if an armed attack occurs' in Article 51. While some might take comfort in the fact that at least the administration is citing international law in some guise, its record of compliance with international law in military security affairs in general is far

---

[4] The Wrong War, August 15 2011, cited at: http://www.nextgov.com/cybersecurity/2011/08/the-wrong-war/49586/

[5] Department of Defense Cyberspace Policy Report, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, November 2011, p. 2 – Cited at: http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf (emphasis added)

from exemplary. In the cyber area in particular, if it was the US that released the Stuxnet virus, then the world already has an example of willingness to violate international law in cyberspace.

Even if the administration's record were better, even if it adhered to the plain meaning of the UN Charter, the relevance of this law to cyberspace may be exaggerated. When cyberspace is conceived of first and foremost as space for communications and economic activity, international law on the use of force is seen by some as largely irrelevant for cyber security. The relevant law is the law governing economic rights and non-intervention, not the law of self-defence. Consider an analogy to chemical weapons: chemicals may be turned into powerful weapons of mass destruction, which defence officials need to plan for, but the non-military sector is where most chemical use and regulation is found. The international community could not tolerate the immensely useful chemical sector being dominated by the military.

Part of the obstacle in persuading governments that the military paradigm is the wrong one for cyber security is the fact that some international law scholars working on cyber security questions from the early days of the internet were in the military or had close ties to it. This is certainly true of the first American authors on cyber security, Michael Schmitt, Walter Gary Sharp and George Walkers. After more than a decade of such analysis, few if any scholars publishing on international law and cyber security do so from a non-military perspective.

This scholarship may well be hardening the view that cyber security is fundamentally military security. Approaching the question from a critical stance, however, reveals that military security authors are relying on attenuated hypothetical cases, not the real world problems of cyber insecurity, crime and espionage. Stuxnet is a real world problem thought to be more obviously in the military defence category, but Iran would not be able to meet several of the conditions of resort to force in self-defence in the case of a response to Stuxnet. The Stuxnet example advocates for a more relaxed reading of international law on the use of force; but there is difficulty in seeing how military force can be resorted to lawfully in response to cyber interference.

International law on the use of force

The argument must begin by reference to Article 2(4) of the UN Charter as the general rule. Article 2(4) generally prohibits the use of force except in the case of self-defence as set out in Article 51 or with Security Council authorization. The World Summit Outcome Document of 2005 restates the international community's support for strict compliance with the Charter rules on use of force.

In addition to the UN Charter, the International Court of Justice (ICJ) in six cases has pointed to important rules of customary international law and general principles relevant to the lawful resort to the use of force. Not only must there be an armed attack or armed attack equivalent to justify the use military force in self-defence, but the attack must be significant; it must be attributable to the state where the self-defence is being carried out; the use of force must be a last resort and must be likely to succeed in achieving defence, and must be proportionate to the injury suffered.

Attempting to apply these conditions to cyber force actions is difficult, if not impossible. Damage to tangible objects occurred only in the case of the Stuxnet attack in Iran. This sort of damage does not meet the condition that an armed attack must be significant to trigger Article 51. As the ICJ said in the *Nicaragua* case: 'The prohibition of armed attacks may apply to the sending by a state of armed bands to the territory of another state, if such an operation, because of its scale and effects would have been classified as an armed attack rather than a mere frontier incident

had it been carried out by a regular armed forces.'[6] The ICJ made similar assessments of 'scale and effects' of violent action in the *Oil Platforms*[7] case, the *Wall Advisory Opinion*[8], and the *DRC v Uganda*[9] case. The Stuxnet attack while unlawful was not the equivalent of an armed attack.

Secondly, attribution has not been affirmed at the international evidentiary standard in any of the three cases. State practice indicates that the case for attribution would have to be made with clear and convincing evidence. In the case of cyber attacks generally, convincing evidence is hard to find:

> Given the anonymity of the technology involved, attribution of a cyber attack to a specific state may be very difficult. While a victim state might ultimately succeed in tracing a cyber attack to a specific server in another state, this can be an exceptionally time-consuming process, and even then, it may be impossible to definitively identify the entity or individual directing the attack. For example, the 'attacker' might well have hijacked innocent systems and used these as 'zombies' in conducting attacks.[10]

Finally, necessity and proportionality may be the most difficult conditions to meet. Estonia and Iran have not even established who attacked their computers. That takes time, and there is a problem of proving that a counter-attack can achieve a defensive purpose. Counter-attacks in self-defence carried out using a computer application will be difficult to limit to the intended target. Over 40 per cent of the computers affected by Stuxnet were outside Iran.

Just because a cyber-attack or cyber espionage do not amount to an armed attack does not mean that international law has no law against such wrongs. Interference with a state's economic sphere, air space, maritime space, or territorial space, even if not prohibited by Article 2(4) of the UN Charter is prohibited under the general principle of non-intervention. This fact is apparent in a number of treaties, UN Resolutions, and ICJ decisions that condemn coercion, interference, or intervention that falls short of the use of force. The ICJ has referred to some of this conduct as 'less grave forms' of force that violate the principle of non-intervention while not triggering rights of a victim under Article 51. In support, the court has referenced the UN General Assembly Declaration on Friendly Relations, the OAS Convention on the Rights and Duties of States in the Event of Civil Strife, and other authoritative sources for the content of the non-intervention principle.

Achieving Cyber Security Lawfully:

What may be done to respond to violations of the principle of non-intervention? What measures are available to respond to CNI lawfully if international law raises substantial barriers to both using cyber weapons and defending cyber space from cyber-attacks through the use of force? In general, international law supports regulating cyber space as an economic and communications sphere and contains coercive means of responding lawfully to cyber provocations of all types. The same

---

[6] Case concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) (Merits), 27 June 1986, para 195. Cited at: http://www.icj-cij.org/docket/files/70/6503.pdf

[7] Case Concerning Oil Platforms (Iran v. United States of America), 6 November 2003, cited at: http://www.iilj.org/courses/documents/CaseconcerningOilPlatforms.pdf

[8] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Request for advisory opinion), 9 July 2004, Summary cited at: http://www.icj-cij.org/docket/files/131/1677.pdf

[9] Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda), 19 December 2005, Summary cited at: http://www.icj-cij.org/docket/index.php?sum=643&code=co&p1=3&p2=3&case=116&k=51&p3=5

[10] David E. Graham, Cyber Threats and the Law of War, Journal of National Security Law & Policy, Vol. 4, p. 92. Also cited, Rick Lehitnen et Al., Computer Security Basics 81 (2d ed. 2006)

sort of coercive measures that are lawful to use against economic wrongs and violations of arms control treaties will generally be lawful to use in the case of a cyber-attack. In the economic sphere, responses to violations tend to be known as 'countermeasures'; in the arms control sphere, they are known as 'sanctions.'

Countermeasures are coercive enforcement measures, not involving the use of significant military force, available to states acting unilaterally in response to an internationally wrongful act. Various arms control treaties, such as the Nuclear Non-Proliferation Treaty and the Chemical Weapons Convention, provide for the Security Council to take action in the case of a violation. The next section provides more details about countermeasures and sanctions, yet, it should be emphasized that despite the availability of these alternatives to the use of military force, however, protecting cyber space, keeping it viable for economic and communication uses, will generally require defensive measures, not offensive ones. Good computer security cannot be replaced by countermeasures, let alone military measures.

Unilateral Peacetime Countermeasures

The international law literature contains little on countermeasures as the lawful response to cyber-attacks. This is likely, as already mentioned, because legal scholars in the cyber security field tend to be divided among those who are expert in domestic internet law issues, especially privacy rights and copyright, and those who come from the world of the international law on the use of force. As noted above, few generalists in international law are writing about internet security. It is not surprising, therefore, that countermeasures are overlooked.

Yet, countermeasures are the mechanisms through which international law allows parties to carry out self-help, coercive enforcement of their rights. Self-help plays a larger role in international law enforcement given the absence at the international level of both a central police force and compulsory courts. The ICJ, in the *Gabčíkovo-Nagymaros* case, laid out four elements of a lawful countermeasure which indicate the relevance of this law to cyber problems:

1. In the first place it must be taken in response to a previous international wrongful act of another state and must be directed against that state.

2. The injured state must have called upon the state committing the wrongful act to discontinue its wrongful conduct or to make reparation for it.

3. The effects of a countermeasure must be commensurate with the injury suffered, taking account of the rights in question.

4. Its purpose must be to induce the wrongdoing state to comply with its obligations under international law, and the measure must therefore be reversible.[11]

If a state is the victim of cyber-interference and has clear and convincing evidence that the wrong is attributable to a foreign sovereign state, the victim state may itself commit a wrong against the attacking state, so long as the wrong is commensurate with the initial wrong (proportionality) and the response is aimed at inducing an end to the initial wrong (necessity) or the provision of damages. In most cases of cyber wrongs, the evidence that a foreign state is behind a particular act will be found only after the act is over or the damage is done. This fact indicates that most countermeasures aimed at cyber wrongs will be a demand for money damages. The

[11] Gabcikovo-Nagymaros Project (Hung. V. Slovk.), Judgement 1997, I.C.J, paras 83-85 (September 25), Quoted in part in Draft Articles, *supra* note 7, Article 49, cmt. 2

international cyber community appears to be adept at estimating the amount of money to repair damage caused by a wrongful cyber event. Thus, a victim state should be able to meet the elements of lawful countermeasures in a way comparable to states suffering trade injuries and having the right under WTO rules to apply countermeasures against the wrongdoing state.

Security Council Sanctions

If cyber-attacks threaten a state's security but do not amount to armed attacks under Article 51, it is also possible for the victim state to ask the UN Security Council to intervene. The Council has imposed sanctions in a variety of situations for decades. It could clearly do so in the case of serious cyber-attacks. To make this clear and to get the benefit of wide notice of such possibility so as to deter cyber misconduct, a treaty spelling out the parameters of lawful and unlawful internet use would be invaluable.

The international community has adopted treaties in other 'dual-use' areas that are analogous to cyber space, such as the Chemical Weapons Convention (CWC) and the Nuclear Non-Proliferation Treaty (NPT). Both of these treaties seek to end any use or even possession of chemical or nuclear weapons while at the same time promoting legitimate non-military uses of chemicals and nuclear power. In the case of both the CWC and the NPT, the Security Council may become involved if states violate the Treaty. In the case of nuclear weapons, the Council has become involved in the case of North Korea's nuclear weapons despite the fact that North Korea has withdrawn from the NPT.

Russia has promoted a treaty patterned on the CWC to regulate cyberspace for a number of years. In a speech on 18th March 2012, Vladislav P. Sherstyuk, a deputy secretary of the Russian Security Council, laid out what he described as Russia's bedrock positions on disarmament in cyberspace. Russia's proposed treaty would ban a country from secretly embedding malicious codes or circuitry that could be later activated from afar in the event of war.

The US, however, was said to have resisted proposals for a treaty. This may relate to US plans to use the Internet for offensive purposes as it is believed to have done regarding the Stuxnet worm. US officials claim publicly that Cyber Command is primarily defensive, but the reluctance to entertain the idea of a cyberspace disarmament treaty is raising questions about the true US position.

Cyber Law Enforcement Cooperation

Whatever the reasons for the US position, drafting a treaty on disarmament and finding alternatives to military force for regulating cyberspace are essential if the internet is to remain available for civilian use. In addition to establishing clear rules for national rights and duties on the internet, a treaty can clarify what is permissible conduct for individuals. A treaty can specify the sort of activity that all states need to regulate through national law and enforcement agencies and in cooperation with other national and international agencies. A model for this part of a comprehensive treaty is already available in the form of the Budapest Convention on Cybercrime.

Good Cyber Hygiene

At the end of the day, countermeasures, sanctions, and even law enforcement cannot substitute for frontline computer and network security measures. An essential step in maintaining a good cyber defence is applying best practices and educating everyone who is legitimately using the internet about safe use. In this respect, the analogy is better made to stopping pandemics than to war or even crime. The internet has made

it easier for hackers to steal information remotely. This is largely due to the proliferation of smartphones.

Governments and organisations will need to find incentives to get cooperation from private corporations and to promote and support international cooperation, especially through international organisations such as International Telecommunications Union (ITU). This might be done by shifting resources away from the military sector to the internet sector, both private commercial and international organisational. Best practices and promotion of a culture of security can be carried out most effectively for the internet through a holistic approach that includes all actors with an interest in maintaining access to a safe internet. The ITU is the natural organisation to lead on common security in cyber space.

Overall, to date, the problem of internet security has been the domain of international law scholars with expertise in use of force questions. They have sent the message that the internet may be lawfully protected through military force or the threat of military force following analogies to the Cold War security strategies. Governments have accepted this modelling, pouring resources into the military to keep the internet safe and to take advantage of what it offers to attack opponents. Doing so has required strained analogies of cyber-attacks to conventional kinetic attacks. The internet is now far less secure than before there was a Cyber Command or a NATO CCDCOE. It is time, therefore, for cyber disarmament and a focus on peaceful protection of the internet. The motto should be: the best cyber defence is good computer defence.

Louise Arimatsu

The cyber 'attacks' we have witnessed to date are primarily, if not exclusively, examples of cybercrime and espionage, not cyber warfare. The use of the term 'battle spaces' is indeed misleading in relation to cyber security more generally. Cybercrime is governed by law enforcement and the term cyber espionage refers to the extraction of data distinct from the threshold of an 'attack' in the context of 'armed conflict'. However, international law is relevant to cyber operations, including international humanitarian law (IHL) and there is a need for development in this area of law. The re-distribution of domestic resources for military purposes in this context is a valid concern.

The Importance of the Law of Armed Conflict in Cyber Operations Security

When a cyber weapon is deployed or implanted, is this something that is quite distinct from a kinetic weapon? Lawyers have struggled with concepts such as 'armed conflict' and 'armed attack' over the years. There is however general consensus that we need to look at the consequences, or in the cyber context, indirect consequences of deploying malware which is regulated by international law.

IHL and *jus ad bellum* (the right to resort to force) are relevant to cyber operations and have a part to play. When the use of offensive digital devices results in injury, death, damage or destruction, the law that governs armed conflict becomes relevant. For example, if country A deploys malware in country B with the aim of destroying critical infrastructure such as civil aviation control and national grids – planes will crash and result in death, injury and damage. If this is caused by digital malware and causes damage to an extent that equates to an armed attack by dropping a bomb on the same targets, there does not seem to be any reason to distinguish the malware from a conventional weapon. To that extent, there is a role for the law of armed conflict.

As we have not yet witnessed cyber warfare of that kind, we are still in the process of understanding how the law applies; it will develop in time, and the law on this issue will become clearer. These two bodies of law (IHL and *jus ad bellum*) are there to prevent conflict and in the event of armed conflict, to restrain parties to that conflict. If we understand how the law applies to potential cyber warfare, we can apply it. It is important for international lawyers to be clear on how the rules constrain all the parties and the need for international lawyers to engage with this question.

One of the main problems is one of attribution. A state is entitled to act in self-defence with regard to an armed attack (kinetic or otherwise). However, cyber presents a particular challenge: to identify who was responsible for the attack.

This problem of attribution, which is not witnessed in other types of warfare, causes difficulties. There are several questions:

1) who is attacking and on what basis?

2) If the attack is by non-state actors, are they getting any state support?

3) 3) If so, what degree of involvement is there?

These questions are important so that we can develop robust rules and are prepared if it does happen in some point in the future. Although the majority of 'attacks' to date are thought to be by non-state actors – (hackers, criminal networks, etc.) – clearly, some will be by states (primarily espionage-related). Non-state actors currently do not have the same capabilities as states. However we need to go beyond the state-state paradigm and think about how the law constrains the use of force by states in the event that non-state actors develop the capability of causing equivalent harm and destruction as states.

Turning to the rules governing armed conflict, cyber capabilities may in fact result in conclusions that are different from what might be expected. For example, in the context of attacks, there is an obligation to attempt to minimise civilian causalities. This raises the question as to whether there is an onus or obligation on technologically sophisticated states to use cyber weapons that will cause less civilian damage than a bomb? Such questions are important and warrant careful consideration.

Discussion

In the context of a discussion about international law on the use of force, it was mentioned that many of the issues could and would be resolved if we had a cyber disarmament treaty. There was need for clarification and communication on what amounts to an armed attack under Article 51 and what would allow a conventional or other kind of attack in response. The internet is a 'dual-use' area and we have to preserve it predominantly for civil and private use; this means we must have clarification in order to restrict and have a set of responses built in when a state considers that it has been injured as a result of another country's failure of due diligence.

A cyber disarmament treaty would be beneficial in developing a defined rule on proportionality and on civilian internet usage. There was a danger of seeing the internet as a space for governments to become more aggressive, attacking others and creating new kinds of weapons. Another need was to elaborate what was required of s' responsibilities in terms of due diligence.

It was noted that the US has now agreed to enter into dialogue with Russia about some codified agreement in this area. However, it was also noted that the

international community should not be under any illusion that the Russian position since 1998 was exclusively to regulate use of this type of 'weaponry' in armed conflict. The text of draft resolutions evidence a very broad understanding of this field and the concern has been that the primary motivation for codification has been to regulate domestic dissent rather than govern international relations.

In response to a question as to the circumstances in which the UN Security Council would regard a cyber attack as a threat to international peace and security it was raised that it is logical to apply the same law as if there had been a kinetic attack. It was argued that in such a case, invoking Article 39 may be more relevant as it is more difficult to attribute the attack. On the other hand, it was explained that while it is possible to analogise a kinetic attack to a cyber attack and apply Article 39 or 51 of the UN Charter, this was still hypothetical.

One participant was interested in thinking about cyber security in terms of economic communications and the issue of counter measures in the economic sphere. It was necessary to return to the international law remedies of retorsion, reprisals, and sanctions. While the WTO system or the bilateral investment treaties system could not be used since they were self-contained regimes with their own specific ideas of counter-measures and sanctions, lessons should be drawn from them. It is important to have some way of measuring compliance and there is a need for monitoring systems.

A point of analogy between cyber and trade sanctions was mentioned: WTO's jurisprudence always has a dollar for dollar amount for trade sanctions, working out the trade injury of non-compliance and putting that on the amount of duty that may be imposed. In the computer network area, there is a lot of understanding about how much damage in a dollar or currency amount may be caused by criminal activity. As a result we can have a concrete idea of economic measures on the basis of how much damage has been done. This was thought to be another argument in the need for a move towards rules governing non-intervention rather than the use of force.

In conclusion, caution was expressed that in today's world, sophisticated malware was being designed by states. There will come a day when non-state actors will have access to malware and we need to understand what the limits are on states when responding to damage on the level of an armed attack. It is important that work is done explaining the ways in which international law limits what states can do in response.