INFOCOMM TRAINING COMMITTEE
STUDY GUIDE

International Regulations On Cyberwarfare

FUNDAMENTAL MODEL UNITED NATIONS @ NUS 2015

14 - 15 February 2015

The Committee

The Infocomm Training Committee (ITC) largely follows the workings of the General Assembly (GA) of the United Nations (UN). Thus far, Economic and Social Council has discussed cyber security, and the Disarmament and International Security Council has debated cyber warfare with the focus on disarmament measures. It is hoped, and of course highly encouraged, that delegates come well-prepared for this committee, going over and beyond what is provided in the study guide.

The Topic

Currently, the world is still reeling from the exploits of the infamous WikiLeaks, and its owner continues to remain on the run after exposing the ugliest secrets of the US government. We also see the acts of the 'online crusaders' Anonymous, who bring down websites and plaster messages in protest of incidents such as the injustices of Ferguson that continues to plague the USA as well as the ongoing assaults in Sudan.

However, beyond these civilian-originated cyberattacks, there lies a more dangerous reality – the imminence of the cyber arms race, and increasingly complicated cyber warfare capacity building. Many countries are taking the hard way to realize the destructive capabilities of cyber arms, while aggressive countries are stealthily yet rapidly capitalizing on these mechanisms to further their political goals and domestic agenda. This includes intense secret developments by China, USA and Russia each of whom have been accused of acts of war in cyberspace, GhostNet, StuxNet and international DoS attacks respectively. These consist large-scale spying, sabotage to physical entities and disruption to crucial economic activities; but barely scrape the surface of the destructive capabilities of cyber warfare.

Armed conflict and military capacities are no longer the defining features of warfare, cyber warfare is able to transcend geographic borders and the prerequisites for conventional warfare. Without a physical attack, offensive cyber capacities are able to capitalize on our reliance on technology, to disrupt key national functions or even destroy critical information systems and societal functions (eg. Financial systems, healthcare facilities).

In light of the increasing threat of cyber war, worsening political tensions, and lack of regulations of cyber arms, how can states coordinate efforts to prevent, identify, and

counter sources of threats and attacks, ultimately stemming any act of war in cyber space?

Key Question

What constitutes an act of war in cyberspace, and how can states coordinate efforts to identify and counter sources of threats and attacks?

Background

Application of International Law

Currently, there exists some resolutions on cyber security and developments in information technology, but the field of cyber warfare remains relatively unregulated. Given the unique characteristics of cyber warfare, it may be difficult to apply existing international law and regulations, such as the UN Charter.

Firstly, it is unclear under what circumstances will cyber-attacks be considered cyber warfare. Only when classified as war, can international law on warfare be applicable. Hence, the cyber-attack has to be qualitatively equivalent to an internationally wrongly threat or use of force, an armed attack that merits self-defense or retaliation. Secondly, the lack of clear territorial boundaries in cyberspace makes it increasingly possible to use other states' cyber capacities and telecommunications infrastructure without prior approval, hence bringing the Law of)Neutrality into question. However, it may be necessary for states to create new neutrality policies relevant to cyberspace, and enforce the protection of its neutrality. Thirdly, if cyber warfare is considered equivalent to armed attack, the International Humanitarian Law may be applicable, though it was designed for conventional warfare. Hence, the extent to which it can be transposed onto cyber warfare remains debatable, such as the regulation of conduct of the belligerents.

Both the military potential and application of existing regulations have not been fully explored, though certain organizations have a recommended set of rules, such as the International Multilateral Partnership Against Cyber Threats (IMPACT).

Unique Characteristics of Cyber Warfare

Cyberspace is the only domain that is man-made in its entirety – it is created, owned, maintained, and used by both the private and public sector, for every purpose imaginable, such as finances/business, healthcare, communication, security, and warfare. As such, though it is readily accessible to all, it is also easily exploited and manipulated.

Although cyber warfare does not utilize weapons of conventional warfare such as kinetic, chemical, biological, and nuclear arms, it does require certain infrastructure and technology. Given the destructive intents and effects of cyber warfare, the used infrastructure and technology may be considered weapons, hence resultant attacks may be considered armed attacks. This has many consequences, as there are various laws concerning armed attacks. However, this classification is highly debatable, because such attacks do not typically cause the ill-effects of conventionally defined armed attacks, such as death and destruction. Instead, the main consequence of cyber warfare is damage to 'critical infrastructure', which a debatable term itself. Though the nuances may differ, 'critical infrastructure' typically consist facilities and systems which when damaged or disrupted, would severely compromise national security and the wellbeing of the people.

Hence, the uniqueness of cyberspace restricts us in transposing existing laws and definitions onto cyber warfare. Though the UN accords each country its right to define 'critical infrastructure', the lack of a standardized definition may heighten the difficulty and complexity of formulating international agreements on the issue.

Key Concepts

Sovereignty in Cyberspace

In cyberspace, belligerents may route their attacks through multiple countries in order to veil the origin of attack, to prevent legal repercussions. The pursuit of cyber-criminals by governments and relevant intergovernmental organizations (eg. IMPACT, INTERPOL, EUROPOL) may require investigation into national information systems and critical infrastructure. The theft of information of cyber-criminals may compromise national security, though the target may be private institutions (eg. Banks).

The aforementioned cyber activities may or may not be offensive in nature, but infringe upon a nation's sovereignty, which may be unjustified since no mass atrocities were committed. Given the lack of geopolitical boundaries in cyberspace, it is unclear on what sovereignty constitutes in cyberspace in the first place. It is then controversial to determine what is 'justified' and how to define/protect sovereignty in cyberspace.

Cyber arms race

Increased international interest in cyber-warfare has sparked the cyber arms race, where countries devote resources to developing cyber offensive and defensive capacities. This modern arena opens the floodgates for stealthier and more destructive attacks, with increased anonymity and control. Its warfare versatility as a standalone complex, alternative to traditional warfare or an integrative complement to current practices results in a rapid cyber arms race and heightened vested interest from certain countries.

> "The logic driving any arms race is the fear that others will get there first (even if there is no clear idea of what "there" may entail) and with enhanced capabilities. Losing the cyber arms race would increase the threats we face—because we already recognize the high level of vulnerability. This destabilizing logic has increased calls for arms restrictions and disarmament in cyberspace."
>
> - Time To Limit The Cyber Arms Race, *Jarno Limnell*

However, the approach to limit cyber capacities would be starkly different from those that limit nuclear and conventional military capacities. Cyber capacities focus on skill, not

infrastructure. Skill is a scarce resource, currently concentrated in select countries, resulting in large disparities.

"Proportionality" in a digital context

Proportionality in law is a principle that is involved in determining "the correct balance between the restriction imposed by a corrective measure and the severity of the nature of the prohibited act". In war, this means that the damages done to civilians and civilian infrastructure must not exceed the anticipated military advantage. Simply putting, the 'punishment/consequence' must match the 'crime'. In a digital contact, it is currently subjective to quantify any attack or military advantage, hence it may be controversial to determine whether the damage done to civilians and civilian infrastructure due to cyber-attacks is 'proportional' to the military objective.

> "While the principle of necessity defines the margins of lawful self-defense in terms of what is objectively necessary to avert or repel an armed attack, the principle of proportionality determines to what extent the harm to be prevented justifies the harm done by the defensive action. From a qualitative perspective, the principle of necessity requires that the self-defensive resort to an otherwise wrongful conduct, normally the use of force, be objectively necessary to avert or repel an armed attack (qualitative necessity)."
>
> - Cyber Warfare and International Law, *Nils Melzer*

USA's Cyber Initiatives and Policies

USA has 5 aspects regarding their defensive strategy for cyber warfare. They are as follows:

1. Treading cyberspace as a domain where territorial sovereignty applies,
2. Active Defense, where sensors respond to attacks rapidly, to trace and take out the intruder/attacker,
3. Critical Infrastructure Protection, where structural integrity of critical and civilian infrastructure is maintained, with a focus on crucial services,
4. Collective Defense, where allies must cooperate to maintain collective cyber security, and
5. Maintaining/Enhancing Advantage, where they constantly develop their cyber capacities to remain at the forefront.

USA also has its Comprehensive National Cybersecurity Initiative, which consists of mutually reinforcing initiatives designed to maintain USA's position at the forefront of cyber security. It is governed by 3 goals, which are as follows:

1. Establish a front line of defense against current threats, through enhancing shared situational awareness of network vulnerabilities
2. Defend against all cyber threats, through building counterintelligence capabilities protecting key information technology
3. Strengthen cyber security, through education, coordinating research and development, and deterring cyber hostilities.

Aspects of cyber attacks

There are generally 4 main aspects of a cyber-attack; they are:

1. Loss of Integrity, where information [which may be confidential and/or sensitive] can be modified improperly,
2. Loss of Availability, where critical information systems or data storages are rendered unavailable to authorized users,
3. Loss of Confidentiality, where confidential and/or sensitive information is disclosed to unauthorized users, and
4. Physical Destruction, where deliberate damage is done on infrastructure through attacks or modifications of information systems.

Key Issues

Defining 'cyber warfare'

Before counter-measures and security policies can be discussed, it is crucial to come to a consensus on the working definition of 'cyber warfare' that embodies the distinguishing factors from mere cyber-attacks. A set of defining criteria would determine if a military response is merited, with a justified amount of physical violence as a counter-measure. Although starkly different from traditional warfare, cyber-warfare has similar repercussions that ripple throughout the global fabric. These include security breaches, collateral damage and other vulnerabilities to politically-motivated malice, which may be incorporated into traditional warfare instead of being used as a stand-alone complex.

Some aspects which can be incorporated into the working definition include the amount of damage to infrastructure and information systems due to the attack, type of attack [eg. Distributed Denial of Service, espionage] and source of attack [eg. Government, civilian, terrorist].

Non-governmental actors

In light of technological advancements, civilians are increasingly able to launch cyber-attacks independent of government authorization. Hence, civilians become active participants of war politics. The nature of traditional war requires the proponents to be states, or groups, with military and offensive capacities. However, in cyber space, attackers are often unidentifiable, and may have capacities insufficient to be determined as an act of war.

For example, patriotic hackers act independent of government control or intervention, though their attacks are politically motivated. They seek to protect or further the interests of their country, by launching cyber-attacks on the country's perceived enemies, through unauthorized means such as launching DDoS attacks on government websites. However, governments may still mask hide their involvement in cyber-attacks to veil their origins by sponsoring the cyber-attack activities of certain groups. This allows the government to act anonymously and attack without inviting retaliation.

Nature of response/counterattack

Cyber-attacks do not have a physical quantifier, as they do not necessarily result in physical damages, hence it is inaccurate to determine the 'justified' amount of retaliation

based on it. When then, would a cyber-attack merit military responses, and to what extent? There exists no international agreements or guidelines on responses to acts of war in cyberspace, so current interpretations are highly subjective.

Due to the current mucky waters, countries may instead choose to develop defensive capacities, which would in turn spark more advanced offensive capacities. Ultimately, this leads to a cyber-arms race, where the aggressive pursuit for offensive and defensive capacities advances the destructiveness of cyber-weapons and integrates into traditional warfare. This includes intense secret developments by China, USA and Russia each of whom have been accused of acts of war in cyberspace. These may include large-scale spying, sabotage to physical entities and disruption to crucial economic activities.

Distinguishing criteria

As stated in the Geneva Convention of 1949, specifically targeting civilian populations is prohibited. The difficulty arises when there is an overlap of civilian and military infrastructure, because the casualties may not be materially obvious. A cyber-attack that damages certain infrastructure for legitimate military purposes, such as electricity supplies and food resources, will also harm civilians significantly.

Also, persons may act collectively without the motivations, lasting affiliation, and hierarchal structures typically characteristic of the adversary groups. Given the anonymity and complexity of cyber-attacks, participation in the hostilities is generally unclear.

Hence, identification of belligerents based on direct participation or membership in certain adversary groups may be inaccurate. Cyber-specific distinguishing criterion would be more appropriate in characterizing the targets of the attacks and identifying sources of attacks.

Espionage and theft in cyberspace

While cyber-warfare has political motivations, cyber espionage/theft are economically motivated, hence must be differentiated as they often do not pose significant military threat. Most theft targets corporate secrets, financial assets, and intellectual property. However, theft of critical information may be seen as a breach of sovereignty, which may be interpreted as a threat to national security and warrant a military response.

Despite the lack of military motivations, espionage still has damaging consequences. The United States Office of the Counterintelligence Executive has reported yearly losses of

billions of dollars due to losses of intellectual property and classified information due to cyber espionage. This report, Foreign Spies Stealing U.S. Economic Secrets in Cyberspace, accredits the aforementioned crimes to state-sponsored actors in China and Russia. Hence, countries with information of tremendous value are at risk of compromises to their network security.

The crux of the matter would be the broadness and subjectivity of the key terms, hence emphasizing the need for a working definition. Countries may manipulate the cyber warfare threat to obscure questionable policies. These policies may include aggressive online monitoring and censorship, under the disguise of protecting civilians and businesses from attacks.

Major Stakeholders

1. International Multilateral Partnership Against Cyber Threats
    a. As a key partner of UN Specialized Agency, the International Communication Union, IMPACT is a politically neutral platform that aims to enhance global cyber security. It is the largest cyber security alliance, and allows stakeholders to collaborate in dealing with cyber threats. Currently, most member states of the UN are also members of IMPACT, though there is uneven participation and contribution.
2. North Atlantic Treaty Organization
    a. NATO has a research and training facility that deals with cyber-security related research and development, consultation, and education – The Cooperative Cyber Defence Centre of Excellence. It has created the Tallinn Manual, a non-legally binding manual on the applicability of extant legal norms on cyber conflicts and cyber warfare. The manual encompasses both the *jus ad bellum* and the *jus in bello*, hence provide a comprehensive approach to the issue. It focuses strictly on cyber-to-cyber operations, such as cyber-attacks on command systems and critical infrastructure, and not on kinetic-to-cyber operations or cyber criminality. However, criticisms to the manual include the impracticability of enforcement, narrowness of its scope, and the infeasibility of various proposed actions.
3. Cyber Offensive Countries
    a. Though countries like China and Russia deny launching cyber-attacks, they are probably the most aggressive countries in cyberspace, using offensive capacities to further their economic and political agenda. Other countries, such as Iran and North Korea, may choose to pursue offensive cyber capacities in order to compensate for perceived military and political weaknesses. Countries like USA have extremely developed offensive cyber capacities, but tend to use them covertly to deal with threats, instead of using them actively an aggressively.
4. Cyber Defensive Countries
    a. For countries facing economic decline, such as certain European countries, cyber capacities pose an additional burden, given the high costs of requisite infrastructure and maintenance of cyber capabilities. Other countries, such as South Korea, are likely to be more concerned with the immediate cyber threats they face from hostile neighbors, namely China and North Korea. Hence, these countries would prefer limiting spread and development of cyber capacities
    b. Countries like Turkey and Egypt are burdened with political instability and social unrest, and use authoritarian measures to restrict social media and

access to the internet in their country. Their main concern would be whether any new laws and policies would interfere with their governance, rather than their vulnerability to cyber warfare. Hence, they would be more supportive of fewer regulations on cyber activities, while still reducing the cyber threats they face.

c. Countries that lack amicable relations with countries that have high cyber capacities would be more concerned with developing their own cyber defensive capacities. More specifically, countries hostile to USA, China, Russia, Iran, etc, would be more at-risk to a cyber-attack. Such countries would prefer the outright elimination of cyber warfare and accumulation of cyber capacities in its entirety, to prevent exploitation by superpowers.

Conclusion

Given the uniqueness of cyberspace and the lack of geopolitical boundaries, cyber warfare has many questionable legal aspects, such as the applicability of existing international law. There are various factors that must be considered when formulating regulations for cyber warfare, such as upholding sovereignty in cyberspace, limiting the cyber arms race, the principles of necessity and proportionality, and the various aspects of cyber warfare. The key issues that must be dealt with include the creation of a working definition, the role of non-governmental and non-state actors, the nature and extent of the response merited by an act of war in cyber space, distinguishing criteria for targets and belligerents, and non-military/politically motivated attacks.

As technology constantly advances and countries rapidly develop their cyber capacities, the disparity between the 'haves' and the 'have-nots' increases, increasing the threat of cyber war. Therefore, it is crucial to establish international law to regulate the spread and accumulation of cyber arms by countries, especially the key stakeholders.

Food for Thought

1. Is cyber warfare a justified alternative to physical violence and conventional acts of war?
2. What is sovereignty in cyberspace and how do we protect it?
3. How do we regulate cyber capacities and prevent the accumulation of cyber arms in any country?
4. How can states be deterred from aggressively pursuing cyber arms development?
5. What is the role of the government in patriotic hacking and how can we prevent/protect against it?
6. Which aspects, and to what degree, should be incorporated into the working definition of cyber warfare?
7. How is government's involvement quantified when non-state actors are involved and what is the government's role in instigating and preventing attacks?
8. Given the lack of a physical quantifier for cyber-attacks, how can we determine the type and extent of response merited?
9. Are cyber espionage and theft part of cyber warfare? If so, how is the economic private sector affected and what is its role?

References

1. World Expo MUN '14 - YaleMUN DISEC: Cyber Warfare Topic Guide
2. SMUN'14 – UNSC: Cyber Security Topic Guide
3. The Economist - Cyberwar: war in the fifth domain
4. WhiteHouse.gov - The comprehensive cyber security initiative
5. McAfee Labs – Time To Limit The Cyber Arms Race, *Jarno Limnell*
6. UNDIR Resources - Cyber Warfare and International Law, *Nils Melzer*
7. Cambridge University Press - Tallinn Manual on the International Law Applicable to Cyber Warfare, *International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*

– MUN for Education, MUN for All –

Co-Organiser:

Main Sponsor: