KleMUN
Kleve Model United Nations

HOCHSCHULE
RHEIN-WAAL
Rhine-Waal University
of Applied Sciences

DISEC

Study Guide – KleMUN 2014

1. Welcome!

Dear Delegates,

We would like to welcome all of you to Kleve Model United Nations (KleMUN) 2014! This November, all of you will have the chance to meet new, interesting people, make friends, debate on recent politics and events, learn about different cultures and get to know the beautiful city of Kleve. In these ever-changing times, with new challenges arising every day, the Disarmament and International Security Committee (DISEC) has to prove its ability to address these problems and to ensure, among others, that global challenges and threats to peace are dealt with accordingly.

Therefore at this year's session of KleMUN 2014, DISEC will be discussing the following topics:

- Piracy upon the Sea
- Usage of Modern Warfare Technology

This study guide will provide a strong foundation for your work for the conference and will form, together with your position papers, the basis of your work.

DISEC will be chaired by Marcus Dörfel, a student of European Studies from Chemnitz University of Technologies who in his spare time he enjoys hiking through Eastern Europe and running a student club and Kristof Verbeke, a 20-year old law student at the KU Leuven in Belgium for whom discussing major topics on a high level and most importantly meeting new people and friends is one of the main reasons he likes MUN's so much.

We hope that you will enjoy the five days of KleMUN 2014, by going through a time of good spirits and shared successes in handling the international communities' problems.

Yours faithfully,

Marcus Dörfel	**Kristof Verbeke**
Chair	*Chair*

2. Background Information

General Information

The United Nations General Assemblies First Committee, the Disarmament and International Security Committee (DISEC) deals with all topics linked to "disarmament, global challenges and threats to peace that affect the international community and seeks out solutions to the challenges in the international security regime"[1].

History

In 1945, when the United Nations was founded, DISEC was created as one of the six main committees of the UN General Assembly. Until 1978 it was called the Political and Security Committee (POLISEC), but was then reformed to the DISEC, as it became clear that a single committee would be overwhelmed by the range of topics. It was then decided that the committee should focus on disarmament. In the times of the Cold War, DISEC quickly became the most important platform for discussions on disarmament, alongside the Conference of the Committee on Disarmament. Caused by the world wide political situation in those years, disarmament, especially concerning nuclear weapons, was highly controversial, and mostly discussed by the nuclear powers. DISEC offered a platform where the non-nuclear states were included into the debates on the matter[2].

Purpose

DISEC shall "consider all disarmament and international security matters within the scope of the Charter or relating to the powers and functions of any other organ of the United Nations; the general principles of cooperation in the maintenance of international peace and security, as well as principles governing disarmament and the regulation of armaments; promotion of cooperative arrangements and measures aimed at strengthening stability through lower levels of armaments"[3].

[1] General Assembly of the United Nations. *Disarmament and International Security.* Retrieved October 25, 2014, from http://www.un.org/en/ga/first/

[2] History Database Search. *First Committee of the General Assembly (United Nations)*. Retrieved October 25, 2014, from http://bit.ly/1ut7Q1d

[3] General Assembly of the United Nations. *Disarmament and International Security*. Retrieved October 25, 2014, from http://www.un.org/en/ga/first/

The General Assembly Resolutions are not legally binding, but as they carry considerable political weight and influence, they usually have enough impact to focus the international communities attention to the topic at hand[4].

3. Topic A: Piracy Upon The Sea

General Information

According to the "United Nations Convention on the Law of the Seas" (UNCLOS), piracy consists of "any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:

> (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
>
> (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;"[5]

Also mentioned in UNCLOS is that all acts, supporting such operations, are regarded as piracy as well.

Contrary to popular belief, piracy not only consists of hijacking a ship or taking the crew as hostages for ransom, but also of armed raids aimed upon stealing provisions and other goods, as can be seen when checking the "Live Piracy & Armed Robbery Report"[6] of the International Maritime Bureau (IMB).

Acts of piracy are most likely to happen in areas where there is little or no control by state actors, as seen at the shores of Somalia[7], where the lack of state control mechanisms enables the pirates to conduct their operations in relative safety or in the Southeast Asian region, where pirates are "exploiting national sea boundaries and the limitations of regional naval forces"[8].

[4] United Nations cyberschool bus. *The General Assembly*. Retrieved October 25, 2014, from http://www.un.org/cyberschoolbus/untour/subgen.htm

[5] General Assembly of the United Nations. *United Nations Convention on the Law of the Sea*. Retrieved October 25, 2014, from http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

[6] ICC Commercial Crime Services. *Live Piracy & Armed Robbery Report 2014*. Retrieved October 25, 2014, from https://icc-ccs.org/piracy-reporting-centre/live-piracy-report

[7] Dua, Jatin (2012). The Context of Contemporary Piracy – The Case of Somalia. *Journal of International Criminal Justice 10* (Oxford, United Kingdom). Retrieved from http://jicj.oxfordjournals.org/content/10/4/749.full.pdf+htm

[8] Business Insider. *Pirates In South East Asia Are Threatening One Of The World's Busiest Shipping Lanes*. Retrieved October 25, 2014, from http://www.businessinsider.com/pirates-in-southeast-asia-are-threatening-one-of-the-worlds-busiest-shipping-lanes-2014-6

Current Situation

After piracy mostly stopped in the 1860s following the Declaration of Paris, which abolished privateering, it returned to a recognisable scale in the early 1990s[9], e.g. in the sea areas around Somalia. In this particular case this became possible by the power vacuum caused by the Somali Civil War. Other hotspots for pirate activities can be found in the maritime areas around the Gulf of Guinea, the Strait of Malacca and the Java Sea[10]. While piracy might be quite common in those areas, there are various differences between the forms of piracy, e.g. the tactics which are used and about the intentions of the pirates. [12]

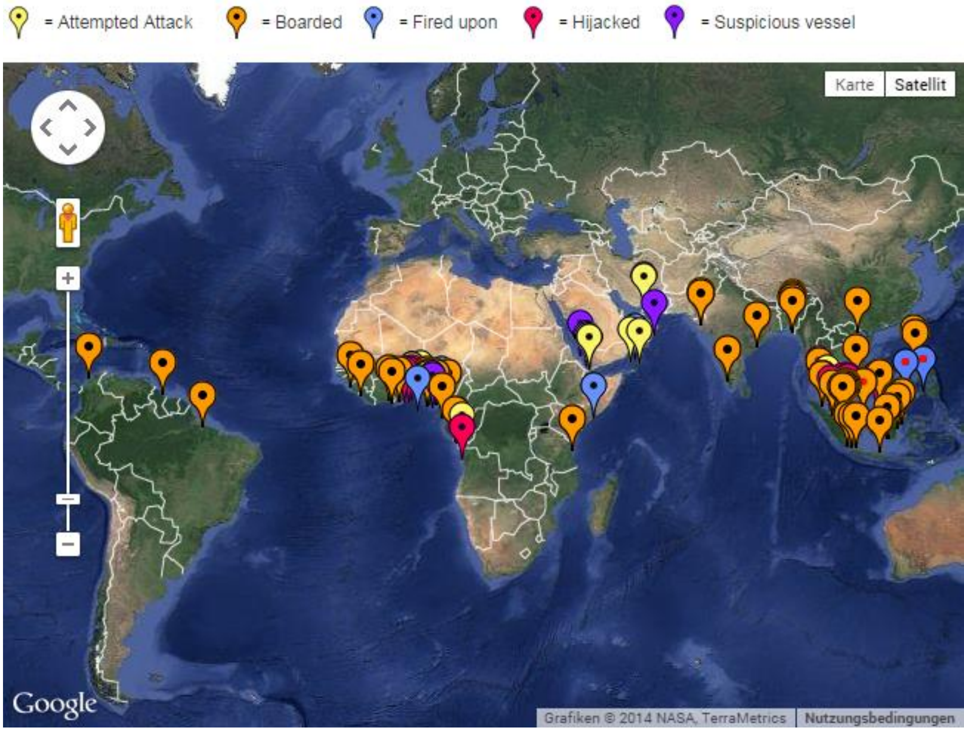


Figure A: Distribution of acts of piracy in 2014[11]

Piracy in East Africa is characterized by daytime attacks (about 75 per cent) on moving ships on the high seas (about 97 per cent), usually involving automatic weapons (about 98 per cent) and aimed upon the hijacking the ships and its crew for ransom.

West African piracy frequently features actions taking place at night (about 60 per cent), tends to focus on ships anchored or lying in port (about 70 per cent), yet no clear pattern emerges about the weapons used, as the whole range of weapons from automatic weapons, explosives, makeshift weapons can be found, alongside totally unarmed raids. The successful attacked ships are usually looted for hostages, their cargo or crew belongings. The level of

[9] Royal Naval Museum. *A Brief History Of Piracy*. Retrieved October 25, 2014, from http://www.royalnavalmuseum.org/info_sheets_piracy.htm

[10] Maritime Connector. *History Of Piracy*. Retrieved October 25, 2014, from http://maritime-connector.com/wiki/history-of-piracy/

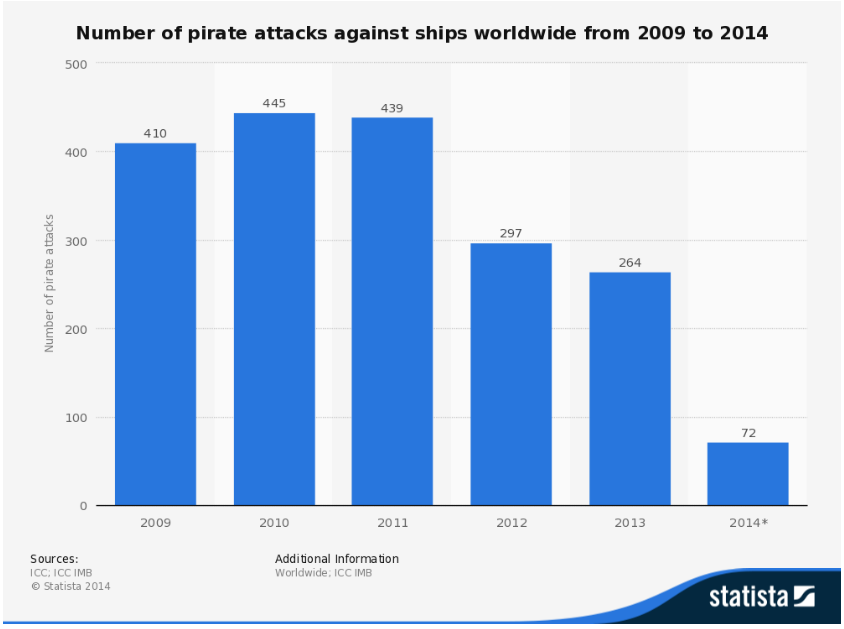
[11] [IMB Piracy & Armed Robbery Map 2014]. Retrieved 2014, October 12, from, https://icc-ccs.org/piracy-reporting-centre/live-piracy-map

[12] ICC Commercial Crime Services. *Piracy & Armed Robbery Prone Areas and Warnings*. Retrieved October 25, 2014, from https://icc-ccs.org/piracy-reporting-centre/prone-areas-and-warnings

violence is the highest compared to the other regions, with about 70 per cent of piracy cases being accompanied by violence. Also the probability of physical violence (about 22 per cent) and the likeliness to be killed (about 9 per cent) is much higher than in other sea areas.

Piracy in Southeast Asia is also focussed on night raids (about 80%), with a balance between moving and stationary ships (about 45 per cent to 55 per cent) and is most likely to include no weapons at all or only makeshift ones (about 85 per cent). The attacks seem to focus on stealing ship equipment or crew belongings.[13]

As can be seen, Somalian/Eastern African piracy is quite different to piracy in other parts of the world. Caused by the daytime attacks in open waters, Somali pirates only manage to successfully board about 10-30 per cent of the ships, whereas non-Somali pirates usually board more than 60 per cent of the attacked vessels. They also focus on capturing ships solely for ransom.[14]



Sources:
ICC; ICC IMB
© Statista 2014

Additional Information
Worldwide; ICC IMB

Figure B: Number of piracy attacks[15]

<u>Response to Piracy</u>

For a successful fight against piracy both the causes as well as the effects must be taken care of. Possible actions against the effects of piracy, meaning the actual attacks, can consist of naval patrols enforced by national maritime forces, either in independent actions in national waters or also with multinational task force, as is happening off the shores of Somalia with Operation Atalanta, to prevent the pirates from reaching their targeted prey. Other actions can consist of hardening the ships against attack and deploying Private Armed Security Companies

[13] Twyman-Goshal, Anamika A. (2014). The Changing Nature of Contemporary Piracy – Results from the Contemporary Maritime Piracy Database 2001-2010. *British Journal of Criminology* (Oxford, United Kingdom). Retrieved from http://bjc.oxfordjournals.org/content/early/2014/05/22/bjc.azu019.full.pdf+html pg. 8-12

[14] Ibid.

[15] [Number of pirate attacks against ships worldwide from 2009 to 2014]. Retrieved 2014, October 12, from, http://www.statista.com/statistics/266292/number-of-pirate-attacks-worldwide-since-2006/

(PASC).[16] Due to different national laws these PASCs are not always allowed in national waters, such as the Nigerian sea areas.

Those actions, however, are not fighting the causes. The situation on the shores of East Africa is deeply linked to the lack of state actors; strictly speaking, the lack of a state. The figures of piracy in that area are closely linked to the beginning of the Somali Civil War.

It seems that permanent monitoring of sea areas could solve most of the problems in West Africa and Southeast Asia, although some problems would still remain unsolved, e.g. the fast operations carried out by Southeast Asian pirates in littoral waters around Indonesia, making use of the confusingly complex archipelagos and the sea borders.

Core Questions To Be Addressed

1. How could the UNCLOS definition of piracy be changed to cover contemporary piracy occurring in territorial waters?
2. How can a sustainable, lasting solution, preventing the causes of contemporary piracy, be assured?
3. What steps must be taken to make the hunt for pirates crossing national sea borders, possible, or to at least ensure a better cooperation between national navy and coast guard services?

Sources & Further Reading

Mandatory reading

Twyman-Goshal, Anamika A. (2014). The Changing Nature of Contemporary Piracy – Results from the Contemporary Maritime Piracy Database 2001-2010. *British Journal of Criminology (*Oxford, United Kingdom*).* Retrieved from http://bjc.oxfordjournals.org/content/early/2014/05/22/bjc.azu019.full.pdf+html

Further reading

[16] Twyman-Goshal, Anamika A. (2014). The Changing Nature of Contemporary Piracy – Results from the Contemporary Maritime Piracy Database 2001-2010. *British Journal of Criminology* (Oxford, United Kingdom). Retrieved from http://bjc.oxfordjournals.org/content/early/2014/05/22/bjc.azu019.full.pdf+html pg. 14

Dua, Jatin (2012). The Context of Contemporary Piracy – The Case of Somalia. *Journal of International Criminal Justice 10* (Oxford, United Kingdom). Retrieved from http://jicj.oxfordjournals.org/content/10/4/749.full.pdf+htm

ICC International Maritime Bureau. *Piracy and Armed Robbery Against Ships – Report for the Period 1 January – 31 December 2013*. Retrieved October 25, 2014, from https://icc-ccs.org/piracy-reporting-centre/request-piracy-report

ICC International Maritime Bureau. *Piracy and Armed Robbery Against Ships – Report for the Period 1 January – 30 June 2014*. Retrieved October 25, 2014, from https://icc-ccs.org/piracy-reporting-centre/request-piracy-report

4. Topic B: Usage of Modern Warfare Technology

Introduction

Contrary to common belief, every war that has been fought out during the past 10 years was also, at the same time, battled over the internet. Cyberwar has become a common occurrence[17], and many countries and organizations, like NATO[18], have noticed an increase in attacks on their systems. The problem is simple: Anyone in the world has access to the internet right now, and with the right knowledge, they can start attacking vital networks all over the world, whether they are private or public. There are a few key reasons[19] why cyber warfare is being practiced more every year. The most important ones are:

1. The internet is vulnerable to attack;
2. There is a high return on investment: There is a rather low cost on getting a knowledgeable person hacking a network, and when they succeed the benefits outweigh the risks by a million. Valuable information about other countries, propaganda, and being able to manipulate data are just a few good return options;
3. The lack of good defence systems against cyber-attacks: At the moment there is a lack of good defence against cyber-attacks. Multiple times the NATO organizations,

[17] See Mandatory reading for examples

[18] NATO, 30 Sep. 2014, Cyber Defence. NATO Newsroom, http://www.nato.int/cps/en/natohq/topics_78170.htm

[19] Geers, K. (2008). *Cyberspace and the Changing Nature of Warfare*. Retrieved from http://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf

when under attack, had to call upon private companies to fix their systems and defend the incoming attacks;

4. The possibility to deny attacks[20]: Cyber-attacks are hard to trace back where they originate from. This makes it nearly impossible to prove a certain country or organization has been hacking into someone else's network since one can never be 100% sure that the right person has been traced. All countries can really do is make claims to one another under the current mainframe. Furthermore even when the country of origin is discovered, there is always the possibility to deny the attack and blame a terrorist organization or an individual person;
5. Everyone can participate, even non-state actors: With the more traditional warfare, usually only the military trained could get involved in the fighting. Nowadays however and specifically applicable to cyber warfare, anyone can get involved. Even lobby groups, or small outcasts can set a cyber-target and make things happen.

Although this topic is still very new on the UN agenda, there has not yet been an official resolution nor definition or treaty that really tackles the problem, it can be seen as DISEC's task to start up a lively debate about this topic.

History of the problem

With the sudden surge and availability of the internet, which started in the 90's, the first known involvements of a two front war came about: one in real life on the ground and one where both sides were sitting in front of a desktop computer. Right now more than two billion users[21] rely in some way upon the internet. It is very interesting to observe how, from the 90's to date,

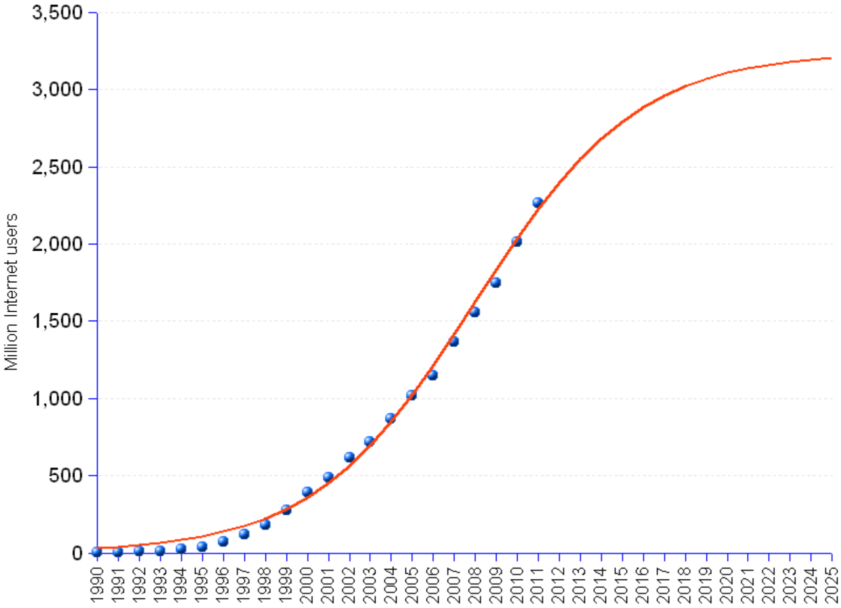


Figure C: A graph showing the increasing number of internet users throughout the years.

[20] Foster, P. (7 May 2013). China denies Pentagon cyber-attack claims. *The Guardian*. Retrieved from http://www.telegraph.co.uk/news/worldnews/asia/china/10040757/China-denies-Pentagon-cyber-attack-claims.html

[21] Data obtained from http://stats.areppim.com/stats/stats_internetxfcstx2012.htm

cyber war did not always have the same purpose or outcome. Some attackers have made use of hacking websites to change their content and send out a message or create propaganda, while others have simply targeted the economy of a country, making it non-operative for a short duration. One of the most common strategies is the DDoS attacks[22], a Distributed Denial-of-Service. In this particular case, the hackers simply flood a network with a whole lot of useless data (for example mails) and makes their server crash. In this way the network and server are rendered useless and especially military wise, communication stops working.

Such an attack at the right time can have devastating means. Nowadays ground and aerial offensives are more and more reliable on information sent via the internet[23].
When a radar system suddenly shuts down, or a target gets overridden, plans can be ruined dramatically.
As an example, a major issue which is feared in the United States is that cyber warfare can also target electricity distribution, say, electricity which all the networks worldwide, and of course most civilians in the world, are dependable on. As former Secretary of Defence Leon Panetta of the US once said: "When it comes to national security, I think cyber warfare represents the battleground of the future.[24][25]" Furthermore, according to European cyber security expert Sandro Gaycken, offensive operations "can, seen from a long-term perspective, potentially cripple economies, change political views, instigate conflicts among or within states and also equalize technological capacities of nations."
Nevertheless, it's not only countries and official organizations which are known to participate in cyber warfare. A big chunk of the pie has been conquered by criminal

[22] For more information on DDoS attacks see: http://s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf

[23] Schimtt N. M., (June 2002). Wired warfare: Computer network attack and *jus in bello*. *IRRC, Vol. 84 N°846.* Retrieved from https://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf

[24] Krepinevich F. A., (2012). Cyber warfare: A "Nuclear option"?. *CSBA report*. Retrieved from: http://www.csbaonline.org/wp-content/uploads/2012/08/CSBA_Cyber_Warfare_For_Web_1.pdf

[25] In regard to this topic see: http://america.aljazeera.com/articles/2014/1/7/defense-leaders-saycyberwarfaregreatestthreattous.html

organizations. Some reports estimate that Eastern European crime groups possess about half of the world's credit card numbers and information[26].

Most of the bigger attacks, like the Aurora attack and Night Dragon[27] are so sophisticated, it is most likely, that a state organised or funded the actions. In April 2011 the South Korean bank got hacked and crashed severely. Even the ATM's were rendered useless for a few days and this had an impact on more than 30 million customers[28]!

However, cyber weapons and attacks still have to prove they are also able to be as devastating as a nuclear bomb. The level of attention cyber warfare has attracted is getting nowhere as close as the studies on nuclear weapons in their first decades of existence. Until an alternative cyber "Hiroshima" emerges, cyber weapons will be used strategically, and seen as annoyance, not as real weapons.

It is DISEC's task however, to anticipate upcoming changes and prevent possible emergency events[29] from happening.

Countries involved

As stated before, anyone can get involved with cyber-attacks. This means both countries and even non-state actors have been part of cyber warfare in some way or the other[30]. It is thus vital that DISEC's tries to act as much as it can on a mutual basis and not a simple majority. With every decision regarding warfare DISEC is taking actions with consequences in all countries and for all their inhabitants. The US, China and Russia however, have reportedly been researching and advancing their cyber involvement throughout the world, as the NSA program and the recent suspected Russian attacks on the NATO[31] potentially prove.

DISEC's involvement

[26] A 2013 report by the Federal Bureau of Investigation states that 781 million US dollar got stolen due to internet crime, and this is only a number thanks to reported cases. For the full report see: http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf

[27] A thorough study on IT security in the Energy industry can be found here: http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/energy-at-risk.pdf

[28] Lee young S., (4 May 2011). Seoul Blames North for Bank Hack. *The Wall Street Journal*. Retrieved from: http://online.wsj.com/news/articles/SB10001424052748703922804576300562037789384?mod=_newsreel_1

[29] Leon Panetta has mentioned "A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack on 9/11"

[30] An interesting blog kept by a McAfee employee mentions more than 40 countries with some sort of Cyber Warfare strategy or training. See: http://blogs.mcafee.com/mcafee-labs/hacking-summit-names-nations-with-cyberwarfare-capabilities

[31] Finkle J., (14 October 2014). Russian hackers target NATO, Ukraine and others: iSight. *Reuters*. Retrieved from: http://www.reuters.com/article/2014/10/14/us-russia-hackers-idUSKCN0I308F20141014

DISEC has not taken decisive action on the topic of cyber warfare. This means the topic should be discussed widely but DISEC should take into account, that addressing the topic through a first resolution is impossible. It might be better to start of the debate about cyber warfare than to complicate matters and block further debates.

Core Questions To Be Addressed

1. Should there be an official definition of cybercrime and warfare?
2. Can a cyber-attack be considered an attack as under Chapter VII and article 2(4) of the UN charter?
3. What can be done to defend states properly against cyber-attacks?

Sources & Further Reading

Mandatory reading

http://time.com/2972317/world-war-zero-how-hackers-fight-to-steal-your-secrets/

http://www.huffingtonpost.com/2014/09/04/hacker-healthcaregov_n_5768494.html

http://www.reuters.com/article/2014/09/18/us-usa-military-cyberspying-idUSKBN0HC1TA20140918

http://www.theguardian.com/world/2014/jun/05/south-korean-databases-hacked-us-general

http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?pagewanted=all

http://news.softpedia.com/news/Russian-Hackers-Suspected-of-Stealing-Documents-Related-to-Ukraine-From-Belgian-Ministry-441826.shtml

Further reading

http://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf

http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF

http://www.csbaonline.org/wp-content/uploads/2012/08/CSBA_Cyber_Warfare_For_Web_1.pdf

http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1198&context=dltr

http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

http://pages.ucsd.edu/~egartzke/papers/cyberwar_12062012.pdf

http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r1110_cyberwarfare.pdf

http://www.un.org/disarmament/HomePage/ODAPublications/OccasionalPapers/PDF/OP19.pdf

https://www.icrc.org/eng/assets/files/review/2012/irrc-886-droege.pdf

http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

https://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf