Committee: Legal Committee

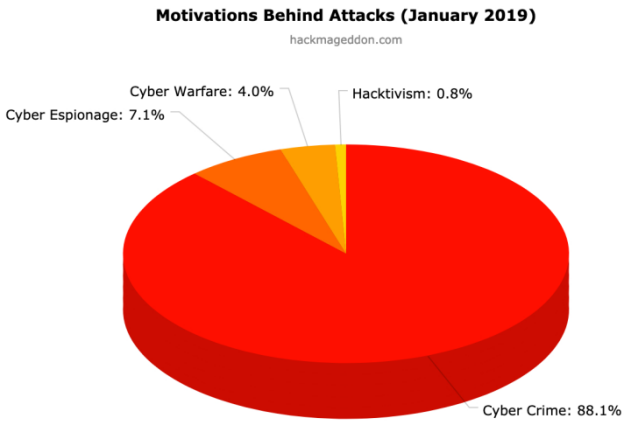
Issue: Establishing a stronger international legal framework on cyberwarfare

Student Officer: Nefeli Pelekanou

Position: Chair

INTRODUCTION

There is no denying that technology is evolving exponentially and this evolution is ameliorating people's lives significantly. As Information Technology (IT) is becoming actively integrated in the economy, government and other important sectors, the digital infrastructure involved in them is becoming major. Unfortunately, the more a state or non-state actor is dependent on its digital infrastructure, the more prone it is to severe disruption of its activities by cyberattacks.



The graph depicts the motives behind cyberattacks reported in January, 2019.

Cyberwarfare is a newly emerging means of warfare that is becoming increasingly frequent with the evolution of technology and its incorporation into crucial sectors of the economy and government. Having accepted that the use of Information and Communication Technologies (ICT) as a means of warfare is an expected consequence of the evolution of technology, it is important to address a number of issues related to its use as a means of offense or defense. There have been no cyberattacks with immense consequences yet, and, for this reason, it is crucial that action is taken proactively to prevent such incidents from taking place in the future.

The UN has deemed the existence of fundamental legislation on all acts of war necessary, in order to prevent the unnecessary suffering of civilians and, therefore, the International Humanitarian Law (IHL) is the official legal document created to set the respective regulations for conventional war. However, due to Cyberwarfare becoming a considerable means of military action very recently, there is a lack of internationally accepted legislation on its utilization, thus making it potentially more dangerous than traditional warfare.

Hence, it is crucial to comprehend that the present matter is not combating cyberwarfare itself, rather than setting the respective legislation on its use in the future, by criminalizing certain activities, similarly to how the IHL regulates the acts of conventional warfare.

DEFINITION OF KEY TERMS

Cyberspace

The internationally connected digital network where communication infrastructures and computer information is available. It consists of domains such as telecommunication networks, the Internet as well as computer systems.

Cyberwarfare

Engagement in activities of conflict or war through cyberspace and by the use of cyber means. More specifically, it is the exploitation of computer technology to cause harm to organizations or states, with a military and/or strategic motive. Cyberwarfare may not only target the disruption of virtual systems, but also non-electronic domains (e.g. power stations or medical establishments, which may have an effect on the lives of civilians)

Cybersecurity

The practice that aims to ensure that a computer system or network is protected from criminal activities, such as cyberattacks and unauthorized collection of computer data.

Cybercrime

The use of cyberspace to carry out criminal activities, such as theft of non-public information. This may include the infection of a computer system with a virus or acts of hacking.

Evolution of cybersecurity

	Then	Now	Impact / Opportunities
Security	Perimeter based	Data based	Mobile /Encryption/ Key Management
Applications	On Premise	SaaS / Cloud	Security-as-a-service
Threats	Static	Dynamic	Event Management / Incident Response
Types of adversaries	Technical chops	Financially / Political motivated	Regulation
Frequency of attacks	??	200 / minute	Monitoring tools
Security Assessment	Periodic	Real Time / Continuous	Vulnerability / Pen Testing
Cyber-security Products	Good enough	Precision, Relevance & Speed	Contextual relevance

The above scheme presents the changes that have taken place in the field of cybersecurity during the past years.

Cyberweapon

Computer software used as a means of warfare in cyberspace. Cyberweapons may include programs that aim at information theft, sabotage, espionage or other activities that belong

to the category of cybercrimes. They are designed to operate without being detected for a specific period of time and require knowledge regarding the potential target so as to bypass cybersecurity measures and carry out the operation.

BACKGROUND INFORMATION

International Humanitarian Law

The International Humanitarian Law (IHL) consists of a number of protocols and guidelines that are to be followed in times of armed conflict and war. The purpose of the IHL is not to stop war per se, rather than to limit the damage caused by it, and protect those not directly involved in its acts (e.g. civilians, the wounded). In other words, it is the international legal framework on *traditional* warfare. The Geneva Convention, which covers a number or matters such as actions that are considered war crimes, is the most widely-known section of the IHL. The IHL could be used as an *analogy* to the legal document that is currently needed for cyberwarfare.

Regarding parts of the IHL that could be applied to cyberwarfare as well, the IHL divides people into three categories:

- The Combatants: The ones who are actively engaged in military activities. They are legally allowed to carry out attacks, but are also in danger of being victims of such by the opposing parties.
- The members of the armed forces that are not Combatants: This includes groups accompanying the combatants without participating in the hostilities (e.g. medical personnel). They have a legal right to protect themselves and their patients but not to attack opposing parties, and they should not be subjects to attacks.
- Civilians: The unarmed population. They do not have the legal right to participate in attacks, and they may not be attacked since they are not taking part in the war.

This distinction is made in order to prevent the unnecessary suffering of civilians during war. Since cyberattacks are capable of influencing civilians' lives as well, even indirectly (e.g. through the disruption of medical or banking services), it is crucial that this aspect is taken into consideration when drafting cyberwarfare legislation. Nevertheless, according to the IHL, not every attack resulting in civilian casualties is considered a breach of the law, only in the case where the casualties outweigh the military advantage expected by the act.

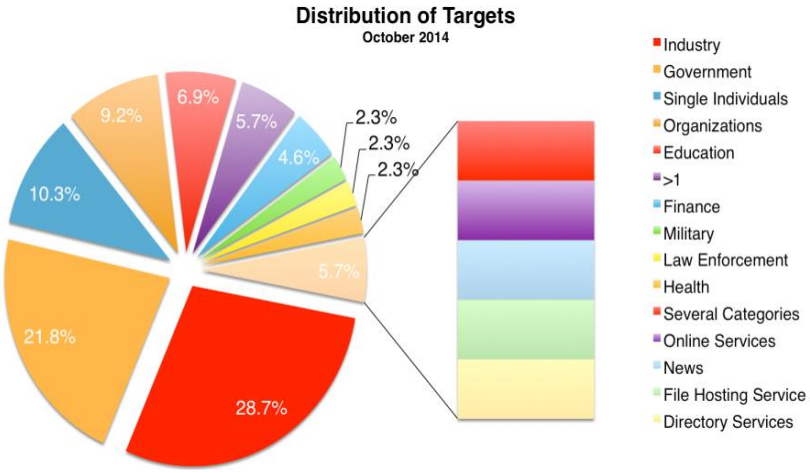
The IHL also comprises of a number of points regarding actions that may occur during war and are deemed unacceptable in its context. Some of them can also be applied in cyberwarfare. These include actions such as false ceasefires and betrayal, the inhumane treatment of non-combatants, attacks on medical units and establishments and attacks aimed at protected individuals or objects.

Major Incidents of Cyberwarfare

The cyberattacks carried out against Estonia in 2007 are possibly the most important ones in the history of cyberwarfare. The attacks were probably politically motivated, as they followed the relocation of a statue dating back to the Soviet era in Tallinn, and were linked to the political conflict between Estonia and Russia, although no entity has taken responsibility for the incident. They lasted twenty-two days and targeted governmental and commercial servers, such as banks, the police, Internet Service Providers, online media, and email services. The results were minimal, such as the temporary loss of governmental and banking services, and there were no long-term consequences. However, although a link to Russia was not proven, the relationship between the two countries was influenced by the events.

One more important Cyber warfare incident took place in Georgia in 2008. After an attack by Georgia on Russian media, there was an attack initially on government websites and news agencies and afterwards on educational and financial institutions, media (such as the BBC and CNN) and a number of businesses. The attacks were carried out through Distributed Denial of Service (a means of cyberwarfare that makes the use of computing systems impossible) and Website Defacement (alterations in public websites). Fortunately, there was no long-term damage that would influence Georgia's sovereignty. The attacks were linked to the Russian Federation; however, the state did not claim responsibility.

The cyberattacks that occurred in South Korea and the United



The graph depicts the sectors that were targeted during cyberattacks, reported in October of 2014

States of America in 2009 are also an important example of cyberwarfare incidents. What is interesting in this case is that the perpetrators are known; therefore, their prosecution is impossible to date. There were incidents of malicious activity; however, again, there were no serious consequences.

What can be inferred by the aforementioned incidents is that Cyberattacks, at this stage, cannot be considered as legitimate acts of war, since no violent events have taken place yet. They are easier to initiate than "traditional" attacks, and since the Internet allows for relative anonymity, it may be deemed quite difficult for the initiators to be detected and prosecuted. Furthermore, cyberattacks are in most cases politically driven, and therefore of the utmost importance, since they have a potential of becoming part of full-scale military operations in the future.

Potential consequences of cyberwarfare

As mentioned, cyberwarfare has not yet escalated to the level where its use will constitute an act of war, although that will possibly change in the future. Over time, digital infrastructure is gradually replacing traditional means of organization and regulation, and more crucial aspects of a state's activities are being conducted through the cyberspace. Such aspects may include the functioning of hospitals, power stations, financial services or fuel provision infrastructure. The fact that in cyberspace it is more difficult for non-combatants to be differentiated from combatants may have negative consequences on the lives of civilians, and, therefore, it is crucial that legislation on cyberwarfare covers these aspects as well.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

Russian federation

The Russian Federation has been very actively involved in the issue of cyberwarfare. Russia is said to have participated in the cyberattacks against Estonia and Georgia, although that has not been proven. Additionally, Russia has deemed the Budapest Convention on Cybercrime (see below) highly invasive in its domestic policies and a potential threat to its sovereignty, and thus it is the only member state in the European Union that has not ratified the Convention. Since Russia is not willing to adhere to the Convention, the permanent representative of the Russian Federation in the UN, along with the permanent representatives of China, Tajikistan and Uzbekistan, have proposed alternative, broader legislation on cyberwarfare.

Estonia

Estonia is one of the leading countries in the digitalization of public infrastructures, since the majority of transactions and interactions between civilians and the government are carried out via the Internet. Therefore, infrastructures that are crucial to functioning of the country are generally vulnerable to cyberattacks. The events in 2007 that were characterized as the first cyberwar, led to Estonia becoming an expert state on cybersecurity. In fact, the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE), which is a center of research and development on cyberwar, is located in Tallinn. Thus, Estonia's experience on the consequences of cyberwarfare and how to address it will be significant in the creation of legislation on warfare.

European Union (EU)

in 2004, the European Union drafted the Budapest Convention on cybercrime, which is the only existing international treaty on the laws of cyberwarfare. It has been ratified by all of the Union's member-states (apart from the Russian Federation) as well as by several non-European member states, and it is believed to be adequate in regard to a legal framework on cyberwar. For that reason, the EU countries are not particularly interested in a new legal document on the issue.

North Atlantic Treaty Organization (NATO)

NATO has declared cyberspace as an environment where its operations may take place, and supports that the International Law applies to cyberwarfare as well. The Organization has been a victim of cyberattacks in the past, and has been cooperating with the EU to ameliorate the response to cyber incidents. A number of its members have carried out cyber operations on behalf of NATO; nonetheless, part of its policy is that each state is responsible for its own actions, even if they were carried out in the context of the alliance, similarly to how each state has its own army and participates in war on behalf of NATO. The aspect of cyberwarfare that is related to ownership of actions in alliances is also one that needs to be addressed in the legal framework on cyberwarfare.

TIMELINE OF EVENTS

Date	Description of Event
23rd November, 2001	The Budapest Convention on Cybercrime was drafted and signed.
1st July, 2004	The Budapest Convention on Cybercrime, drafted by the Council of Europe entered into force.
27th April, 2007	The cyber attacks against Estonia commenced and lasted approximately twenty two days.
20th July, 2008	The cyber attack against Georgia began.
July, 2009	The cyber attacks against South Korea and the United States of America occurred.
1st October, 2010	The UN Group on Cybercrime and Cybersecurity was founded during the 20th session of the UN High-Level Committee on Programmes
12th September, 2011	The permanent representatives of China, the Russian Federation, Tajikistan and Uzbekistan drafted a letter to the United Nations aimed at the Secretary General proposing an alternative to the Budapest Convention.
10th December, 2014	The draft policy on cybercrime and cybersecurity by the aforementioned UN Group was ready for approval.

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES AND EVENTS

Although the UN has not yet taken action on the establishment of legal framework on cyberwarfare, there has been internal activity that aims at its active engagement on the matter.

Document A/66/359[1]

Since a number of member states were not willing to adhere to the Budapest Convention on Cybercrime, the permanent UN Representatives of the Russian Federation, China, Uzbekistan and Tajikistan drafted a letter addressed to the Secretary-General of the United Nations on 12th September, 2011**.** The letter proposed alternative legislation on the use of information and communications technologies that is consistent with the states' policies. It is open for states to adhere to but not obligatory.

It encourages compliance with the UN Charter, with focus on human rights and respect to every state's independence. It proposes that information and communications technologies should be used neither for hostilities nor any other action that challenges any state's peace

[1] https://undocs.org/A/66/359

and security and furthermore that the production of cyber weapons should not take place. It also aims to protect states' social, cultural, economic and political environment from terrorist or criminal activities through cyberspace, and urges states to strive to prevent such incidents initiated by other states as well. The rights and responsibilities to protect from attacks are, however, reaffirmed by the letter's proposal, as well as free browsing in cyberspace. Efficient Cyber Governance is endorsed, as a means of fair Internet management. Finally, the development of a culture of digitalization and information security is highly encouraged, both in developed states as well as in developing, with the assistance of More Economically Developed Countries (MEDCs).

A letter is not a resolution, which means that it has not been voted on by the General Assembly; however, it consists of the proposals made by the aforementioned countries as to which points the international legal framework on cyberwarfare should cover.

UN Group on Cybercrime and Cybersecurity

In 2010, the UN High-Level Committee on Programmes (HLCP), which is a commission that discusses and acts on important matters in several sectors, during its 20th session, emphasized the importance of a framework on cyberwarfare, and for that reason, set up a UN Group on Cybercrime and Cybersecurity. The aim of the group is to create a policy on cybercrime. Since then, there has been a draft framework; nevertheless, the HLCP has not reported progress since its 28th session which took place in December of 2014, when the draft was ready for approval.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

Even though there have been attempts by independent parties to regulate the use of cyber weapons, there is still a lack of a legal framework with international acceptance, since a number of states refused to adopt the proposed policies.

Budapest Convention on Cybercrime[2]

The Budapest Convention on Cybercrime was drafted by the Council of Europe and entered into force in 2004. It is the first international attempt to create a legal framework on cybercrime and its aim is to promote the creation of international, as well as domestic

[2] http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

cybercrime policies based on fundamental principles by criminalizing actions that should not be tolerated in cyberspace.

Briefly, through the Budapest Convention, states are urged to criminalize the intentional unauthorized access to computer systems, as well as the interception of digital signals transferring data. Furthermore, the Convention condemns the interference of any means, on computer data and systems without the respective right, as well as the distribution of any means of data that can allow access to such systems with the intention of committing any of the aforementioned actions. The falsification of data is also criminalized, along with actions that result in one's loss of personal property. Child pornography produced and used in any way is also denounced. The Convention asks states to actively prosecute such actions.

States are, however, given the right to require specific conditions such as, but not limited to, dishonest motive or considerably harmful consequences, to prosecute such actions. This measure makes the convention more adaptable to the domestic policies of each state.

Budapest Convention as a guideline

Example: Loi relative à la cyber sécurité et à la cybercriminalité au Cameroun (2010)

Article	Budapest Convention	Law of Cameroon
Art. 7	Computer-related forgery	Article 73
Art. 8	Computer-related fraud	Article 72
Art. 9	Child pornography	Articles 76, 80, 81
Art. 10	IPR offences	
Art. 11	Attempt, aiding, abetting	
Art. 12	Corporate liability	

www.coe.int/cybercrime

The scheme presents some of the important aspects covered by the Budapest Convention on Cybercrime, and the articles in which they are analyzed.

The present Convention is fully supported by the European Union (EU); however it was deemed invasive by states such as the Russian Federation, China and India, who refused to ratify it in its present form. The aforementioned states request a UN Resolution on the matter, although the EU considers the Budapest Convention sufficient and is not in favor of further negotiations[3].

On a general note, when a Convention is ratified by a state, it becomes legally binding, which means that the state is under international legal obligation to adhere to the articles included in the Convention. Establishing a strong international legal framework on cyberwarfare requires that most states, and especially those of greater political and economic dominance, are willing to adhere to its guidelines, something that the Budapest Convention did not achieve.

[3] Full list of states related to the Budapest Convention and their stance towards it: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

POSSIBLE SOLUTIONS

The present issue is the lack of an internationally accepted legal framework on cyberwarfare. Therefore, the solution is the creation of one, and the resolutions that will be drafted should not focus on how states will decide on a legal framework, rather than act as the legal documents themselves, expressing policies on cyberwarfare.

As mentioned previously, the states that have ratified the Budapest Convention on Cybercrime are not keen on drafting a new policy on cyberwarfare, since they think that the Convention is adequate. Therefore, it is expected that such states will propose policies similar to the ones mentioned in the Budapest Convention. The Budapest Convention is more specific, covering aspects such as illegal access to computer systems, interception of signals, alteration of data and systems, child pornography and copyright violations. One could say that the Budapest Convention is specific and relatively invasive to the states' domestic legislation.

On the contrary, the letter addressed to the UN Secretary-General, which, even though it is not officially a legal document, reflects another stance on cyberwarfare, is less rigid and more adaptable to a state's domestic legislation and policies. In that case, the adherence to the UN Charter is a basic requirement for the resolution of this stance, as well as the principle of refraining from using information technology in the conduct of hostile activities. The main point that differentiates this stance to the one expressed by the Budapest Convention, nevertheless, is that in the legislation proposed by the letter, emphasis is applied to "information security", rather than simply "cybersecurity", which apart from the regulation and protection of computer networks and systems, also includes the regulation of information content. Therefore, actions that derive from the free flow of information in cyberspace and violate state laws, constitute cybercrimes (e.g. the use of social media for that purpose), according to that policy, whereas states that support the Budapest Convention consider the free flow of information a basic right. The policy also emphasizes the role of states in combating cyberattacks, by reaffirming and focusing on the fact that states have the right and obligation to protect against threats to their sovereignty and security and the fact that this principle also applies to cyberwarfare. Hence, these points should be taken into consideration when drafting a resolution.

Regardless of the policy on cyberwarfare, the legal framework should take into account the IHL and its principles, as well as the fundamental UN polices, since the law of armed conflict

applies to cyberwarfare as well. A legal document, in order to be accepted by as many states as possible, has to combine the aforementioned stances effectively.

BIBLIOGRAPHY

"Action on Cybercrime and Cyber Security." United Nations System, 3 May 2013, www.unsystem.org/content/action-cybercrime-and-cyber-security.

"Action on Cybersecurity." Action on Cybersecurity | United Nations System Chief Executives Board for Coordination, 10 Jan. 2010, www.unsystem.org/content/action-cybersecurity-0.

Arimatsu, Louise. A Treaty for Governing Cyber-Weapons: Potential Benefi Ts and Practical Limitations. 2012, ccdcoe.org/uploads/2012/01/2_3_Arimatsu_ATreatyForGoverningCyber-Weapons.pdf.

Ashmore, William C. "Impact of Alleged Russian Cyber Attacks ." School of Advanced Military Studies United States Army Command and General Staff College , nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-027.pdf.

"Building a Stronger International Legal Framework on Cybercrime." Chatham House, 7 Dec. 2018, www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime.

"Chart of Signatures and Ratifications of Treaty 185." Council of Europe , 19 June 2019, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

"Cyber Weapon ." Macmillan Dictionary, Macmillan Dictionary, www.macmillandictionary.com/dictionary/british/cyber-weapon.

"Cybercrime." Lexico Dictionaries | English, Lexico Dictionaries, www.lexico.com/en/definition/cybercrime.

"Cybercrime." Oxford Learners Dictionaries, www.oxfordlearnersdictionaries.com/definition/english/cybercrime.

"Cybersecurity ." Lexico Dictionaries | English, Lexico Dictionaries, www.lexico.com/en/definition/cybersecurity.

"Cyberspace ." Lexico Dictionaries | English, Lexico Dictionaries, en.oxforddictionaries.com/definition/cyberspace.

"Cyberwarfare ." Lexico Dictionaries | English, Lexico Dictionaries, en.oxforddictionaries.com/definition/cyberwarfare.

Hakmeh, Joyce. “Building a Stronger International Legal Framework on Cybercrime.” Chatham House, 6 June 2017, www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime.

“How Estonia Became a Global Heavyweight in Cyber Security - e-Estonia.” e-Estonia, June 2017, e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/.

“Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General .” UN General Assembly, 14 Sept. 2011, undocs.org/A/66/359.

Melze, Nils. “Cyberwarfare and International Law.” UNIDIR Resources, 2011, unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

“NATO Cyber Defence.” North Atlantic Treaty Organization, Feb. 2019.

Nato. “Cyber Defence.” NATO, 16 July 2018, www.nato.int/cps/en/natohq/topics_78170.htm.

Ottis , Rain. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

“Regional Courses in International Law.” Legal UN, 2017.

Shakarian, Paulo. “The 2008 Russian Cyber Campaign against Georgia.” Military Review, U.S. Army CGSC, 1 Nov. 2011, www.questia.com/library/journal/1G1-273195159/the-2008-russian-cyber-campaign-against-georgia.

“Significant Cyber Incidents.” Center for Strategic and International Studies, www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

Weaver, Matthew. “Cyber Attackers Target South Korea and US.” The Guardian, Guardian News and Media, 8 July 2009, www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack.

“What Is Cyber-Security?” Kaspersky, www.kaspersky.com/resource-center/definitions/what-is-cyber-security.

Wilson, Clay. “Cyber Weapons: 4 Defining Characteristics.” GCN, 4 June 2015, gcn.com/articles/2015/06/04/cyber-weapon.aspx.

“Convention on Cybercrime.” Council of Europe, 23 November 2001, rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000001680081561

Uchenna Jerome Orji, “Russia and the Council of Europe Convention on Cybercrime.” Nnamdi Azikiwe University, January 2012,

www.researchgate.net/publication/322083052_Russia_and_the_Council_of_Europe_Convention_on_Cybercrime

"The United Nations, Cyberspace and International Peace and Security."UNIDIR, UNIDIR Resources, 2017, www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf

Hjortdal, Magnus. "China's use of Cyber Warfare: Espionage meets strategic deterrence", Journal of Strategic Security, 2011, www.jstor.org/stable/26463924?seq=3#metadata_info_tab_contents

Farnsworth, Timothy. "China and Russia Submit Cyber Proposal." Arms Control Association, www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal.

Eichensehr, Kristen. "International Agreements-and Disagreements-on Cybersecurity." Just Security, 24 Oct. 2014, www.justsecurity.org/16706/international-agreements-and-disagreements-on-cybersecurity/.

Multimedia Resources

https://www.google.com/url?sa=i&source=images&cd=&ved=2ahUKEwi7ype1iofjAhWB_aQKHbKeBMUQjRx6BAgBEAU&url=https%3A%2F%2Fwww.privacyrisksadvisors.com%2Fdata-breach-toolkit%2Fworlds-biggest-data-breaches%2F&psig=AOvVaw3OsWf9ZbGGrn7UkSZXmF5A&ust=1561636185470334

https://www.hackmageddon.com/wp-content/uploads/2019/02/Featured-Image-Statistics.png

https://slideplayer.com/slide/5296739/17/images/7/Evolution+of+cybersecurity.jpg

https://image.slidesharecdn.com/ctocybersecurityforum2013alexanderseger-budapestconventiononcybercrime-130704083741-phpapp02/95/cto-cybersecurity-forum-2013-alexander-seger-budapest-convention-on-cybercrime-11-638.jpg?cb=1372998201