Forum:	Disarmament and International Security Committee
Issue:	Establishing an international framework on Cybersecurity, Human Networks and Artificial Intelligence
Student Officer:	Kassiani Beleri
Position:	Co-chair

PERSONAL INTRODUCTION

Dear delegates,

My name is Kassiani Beleri and I have the extreme honour to serve as a co-chair in the Disarmament and International Security (GA1) committee of the 8th session of PSMUN. I am seventeen years old and I attend the 11th grade of the Anavryta Model Lyceum, a state high school in Greece. PSMUN is going to be my eleventh conference and third time chairing, the first time however, chairing in a General Assembly committee.

In this study guide I have chosen to mention many aspects of technology and the dangers its usage poses to humans. As I came to find out, the maintenance of cyber security is a very broad issue, as cybercrime consists of many violations. I am sincerely hoping that my study guide will help you in your research, provide you with significant information and also give you some ideas when it comes to writing your resolution.

INTRODUCING TOPIC

Establishing an international framework on Cyber Security, Human Networks and Artificial Intelligence, as an issue discussed in the Disarmament and International Security Committee brings forward the occasion of technology actually threatening the peace and security of the civilians, the states and the international community. Technology undoubtedly has significant advances, but also poses great risks to its users.

For one thing, there seem to be more and more new trends in cybercrime, which bring forward the need for more effective international cyber security. Moreover, the very existence of human networks and the latest developments in the field of Artificial Intelligence need to be addressed by the international community.

KEY TERMS

Cybercrime[1]

The term refers to any Internet-related criminal action. Cybercrime is divided into two main categories:

- *Advanced (high-tech) cybercrime*, which defines the attacks against computer software and hardware
- *Cyber-related crime*, which includes any form of 'traditional' crime committed partly or entirely via the Internet

Hacking

"The activity of illegally using a computer to access information stored on another computer system or to spread a computer virus."[2]

Malware (malicious software)

Any computer program designed to harm the legitimate user of a computer. [3]

Ransomware

An insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them.[4]

[1]There is not an international term defining cybercrime. The above definition is from INTERPOL, however wording of the definition of cybercrime of other international governmental or security organizations may vary.
[2]Cambridge Advanced Learner's Dictionary & Thesaurus
[3]INTERPOL
[4]Federal Bureau of Investigation (FBI)

Spyware

Malware that once it infects a device it is able to monitor its activity and transmit the information.

The Deep Web(Dark Net)

The part of the Internet that is not accessible via search engines. The Deep Web includes information that is password-protected and websites that use specialized software and anonymity tools, therefore its users are hard to detect. Criminal activity in the Dark Net is mainly black-market weapon sales, drug sales and child abuse streaming.

Money laundering

Any act or attempt to disguise illegal profit, so that it appears to have legitimate sources, in order to avoid suspicion and incrimination.

Counterfeiting money

Unauthorized production of currency.

Human trafficking

"*the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs*"[5]

Artificial intelligence (AI)

"the study of how to produce machines that have some of the qualities that the human mind has, such as the ability to understand language, recognize pictures, solve problems, and learn"[6]

Human network

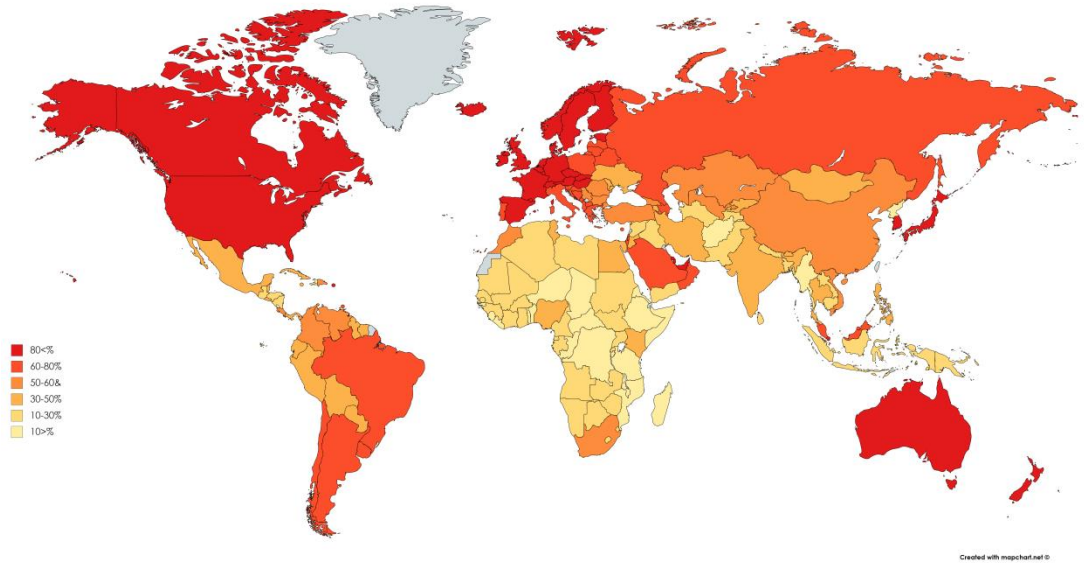
A group of people that communicate with each other via technology means.

[5] Article 3 of the Protocol to Prevent, Suppress and Punish Trafficking in Persons of the UN
[6] Cambridge Advanced Learner's Dictionary & Thesaurus

HISTORICAL INFORMATION

Cyber security

The Internet was born in the 1960s. Back then, it was called ARPANET and consisted of a small network of computers that could talk to one another, used by the Americans, so that their communication wouldn't be detected by the Soviets during the Cold War. By 1969, ARPANET was formed by solely four computers and messaging among them faced many difficulties. However, after many scientists' efforts, it evolved and during the 1980s was used for the exchange of files and data between researchers. In 1991 the World Wide Web was created and ever since, it has been accessible to billions of people and the number keeps growing.



The percentage of the population per country who are Internet users. From darkest to fairest color: 80< %, 60-80%, 50-60%, 30-50%, 10-30%, 10> %

Throughout its development the Internet has been a stunning invention and, in many ways, has shaped the world as we know it today. But unfortunately, it has also created the need for what is called cyber security. Cyber security means taking measures for the protection of the users of the Internet and against offences and crimes occurring in or through cyberspace. Cybercrime is ever-growing.

Advanced cybercrime

Advanced cybercrime includes the techniques hackers use to attack hardware and software. Advanced and cyber-related cybercrime are connected to each other as usually in order for a traditional crime to be committed through the web, hacking is needed.

The main advanced cybercrime attacks are:

- Malware

Malicious software is used for a wide range of criminal activities including data theft, obtaining personal information, disrupting a system and monitoring a system.

- Ransomware

Ransomware is currently the newest trend in cybercrime, as ransomware attacks are becoming more and more sophisticated. These attacks target hospitals, school networks, companies, small businesses, networks of a state, a government and law agencies. Ransomware is related to fraud.

- Bots, botnets

A botnet is created when the malware that has infected a device allows the cybercriminal to have complete control over it. Botnets can be used in many ways such as massive sending of spam e-mails and downloading or distributing other malware.

Other types of malware are rootkit, worm, trojan, file infector, backdoor/remote-access trojan (RAT), scareware, spyware and adware. [7]

Cyber-related crime

- Fraud

Fraud includes all the tricks criminals use to deceive and manipulate people into giving out confidential information and sums of money. There are several types of cyber fraud. It is committed through email hacking, when someone hacks the email of an individual and asks their contacts for money or information and through email pretexting and phishing. Pretexting is when someone creates a scenario, e.x. the impersonation of a bank officer, and approaches their victim via email, whereas phishing means that there is a group of people doing the pretexting. In addition, fraud is accomplished via online sweepstakes and lotteries and email spam.

- Identity theft

Identity theft is when a cybercriminal hacks the Internet accounts of an individual and uses their personal and/or financial data. An example of this is the draining of one's money in a credit card. In the broader spectrum, identity theft is also the hacking of a firm's data in the Internet for similar reasons.

[7] A full list of the explanation of all the types of malware mentioned:https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

– Digital piracy

In other words, copyright infringement. The illegal duplication of copyrighted works such as music, videos and books and their unauthorized provision in the Internet has been a major cybercrime trend of the 00s that exists to this day. Digital piracy is actually very extensive and although the shutting down of piracy websites may not be that difficult to achieve, the handling of online copyright infringement is a challenge, exactly due to the fact that it happens very often. The immediate victims of the violation of copyrights are the creators of copyrighted works and their partners.

– Money laundering & counterfeiting

The Internet in many ways has made money laundering easier. According to a research of the US Department of State, 16.9% of money laundering is done via computer intrusion, meaning the gaining of access to unauthorized data in the Internet. Moreover, money laundering is enhanced by anonymity and identity theft. Websites that allow transactions without requiring the personal information of their users, can be and are often used for money laundering.

Counterfeiting which acquires 7.9% of the world's money laundering can also happen online. Some online-shopping websites trick their customers by providing them with products that are not qualified for their price and frequently enough this immense profit eventually ends up being counterfeit money.

– Trafficking

Trafficking in persons is often related to cybercrime. Traffickers use the web to interact with their potential victims, or worse recruit them through social media and sell the services they force upon them through the Deep Web. There are currently approximately 20,9 million victims of trafficking in the world, among them many children that are being sexually exploited.

– Child sexual exploitation & abuse

The sexual exploitation and abuse of children on the Internet is accomplished both through the clear internet and Dark Net forums. It is a very sensitive issue and its combat has been a priority of the United Nations Office on Drugs and Crime (UNODC). Child sexual abuse online means that the abused is forced to either post sexually explicit images of their body, participate in sexual conversations through chatting forums, or engage to sexual activities via webcam or smartphone. Moreover, young persons under the age of 18, also bear the threat of being victims of online sextortion, which means they are being blackmailed to perform the aforementioned activities. Lastly, in the Deep Web there is extensive streaming of children being sexually violated, which brings forward many issues that have to be resolved, such as how the molester got in touch with the victim in the first place, which is usually through trafficking.

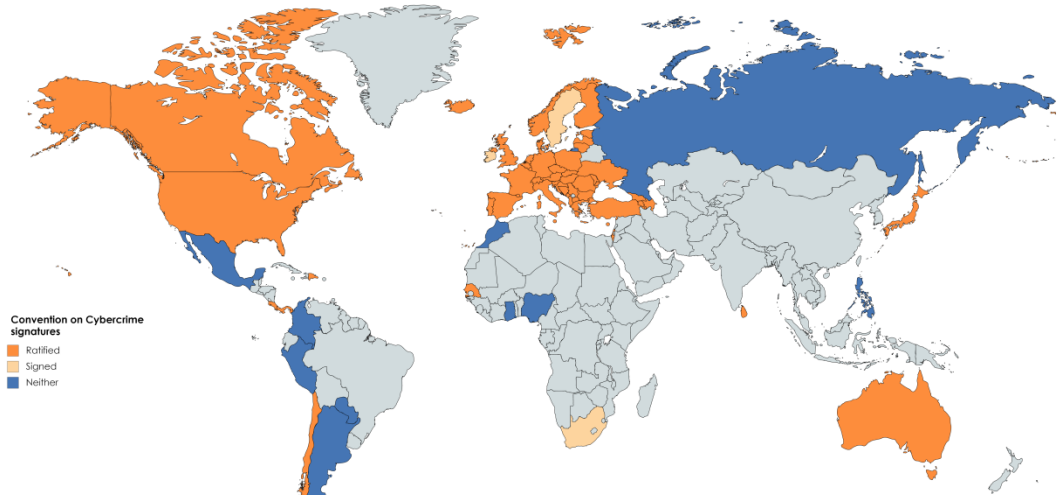
– Espionage

Cyber spying is the monitoring of an individual's or a company's data on the internet without their knowledge and sending them to a third party and therefore is considered to be a flagrant violation of privacy. Government surveillance, whether it is a government spying on its people or a government spying on another government, also lies in this category.

– Terrorism

Cyber terrorism is terrorism conducted through cybercrime. In other words, it is the usage of cyber-attacks as a way of forcing the government and its people to engage to the terrorists' political and social objectives. Most of the time cyber terrorism also involves threat of loss of human life and destruction of infrastructure.

Two of the most important initiatives for the reduction of cybercrime are the Budapest Convention on Cybercrime and the Virtual Forum Against Cybercrime. In 2001 in



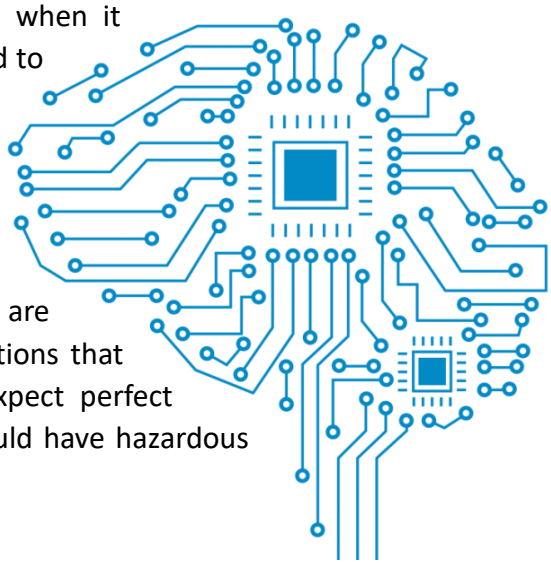
The signatures of the Convention of Cybercrime. In orange: countries who ratified, in light orange: countries who signed, in blue: countries who did not sign or ratify

Budapest the Council of Europe adopted the Convention on Cybercrime, which is the first and to this day most significant agreement that addresses cybercrime. The VFAC was created in 2005 by the Korean Institute of Criminology in cooperation with the United Nations. Its main aims are to provide information and training to law enforcement personnel regarding cybercrime.

Other organizations that contribute to the research of cybercrime are the United Nations Office on Drugs and Crime (UNODC),the International Police(INTERPOL) and the European Police Office (EUROPOL).

Artificial intelligence (AI)

AI suggests that machines keep improving their performance without needing humans to give them detailed instructions for every task they have to accomplish and as these systems are often excellent learners, they can achieve superhuman capacities. Currently AI is in use in thousands of companies around the globe and the number is to keep growing. Among the many fields, AI provides and is bound to provide assistance, are education, transportation, manufacturing, health, law and insurance.



There comes, however, a lot of questioning when it comes to its apply. It is argued that AI can lead to the increase of world-wide unemployment, as it replaces human workforce and that its high costs may well result to the deprivation of its benefits for a large group of people. Another issue is the amount of "trust" people should actually put on AI. As the data put in AI are usually imperfect or cannot predict complications that may occur, it would be wrong to always expect perfect results. Therefore, extreme reliance on AI could have hazardous effects.

In June 2017 the United Nations' Secretary General, António Guterres, reminding the benefits of the vast development of AI, stated that the UN should make good use of it with aims to eliminate poverty and hunger. He did, however, also mention that there are also ethical issues and challenges in its usage, with reference to human rights and privacy and cybersecurity.

Human networks

Human networks are platforms that accomplish the secret communication between groups of people. They are often used between a company's officials, so that they get to communicate on their plans and decisions regarding their working environment. In such prospect, human networks can be very beneficial and provide significant help in a company's management.

Their usage is, however, questionable as to what extent human networks shall maintain their secretiveness. The reason for this is that there is the case of communication in the networks exceeding other employees for equal and fair participation in a company's affairs and eventually poses discrimination between colleagues.

COUNTRIES INVOLVED IN THE ISSUE[8]

African countries

In comparison to the world the African continent has a very small percentage of Internet users. This, however, does not mean that its citizens are not threatened by cybercrime. On the contrary, many African countries deal with severe human trafficking, child exploitation and inter-state terrorism, which are also supported by cybercrime tactics. When it comes to addressing these transnational issues, some states believe that cyber security is pivotal for their confrontation, while many others maintain a neutral policy and are not actually supportive.

European countries and the European Union(EU)

Inside the EU's framework, cybercrime is a largely addressed issue. Between the European countries there has been cooperation and measures have been taken to deal with cyber threats, such as the creation of the Convention on Cybercrime of the Council of Europe. Unfortunately, cybercrime thrives in Europe and that is because the vast majority of Europeans and especially young people are Internet users. In general, the countries of Europe are for the development and broader application of cyber security.

Countries of the Middle East and Asia

Although in Asia and the Middle East statistics of Internet usage vary from country to country, the greater picture shows that a large number of people bear the threat of being victims of cybercrime. In many of these countries, the national governments censor parts of the Internet so as to ensure the safety of their citizens. Of course, internet censorship covers a much broader spectrum and may be done for plenty other

[8]The subheadings in this section only propose a general picture. Policies among countries of course vary.

reasons. However, these same countries often argue that in order for cyber security to be achieved, a censorship policy could be obtained.

North and Latin America

Once again, as there are many people who use the Internet in these countries, maintenance and strengthening of cyber security is to them essential and they promote cooperation and action against cybercrime. In the U.S.A., the Federal Bureau of Investigation(FBI) spends a considerable sum of money combating cybercrime, also assisting the international community. In the Americas, the occurrence of cybercrime is very common and activity in the Dark Net seems to be significantly increased, as there is a lot of drug and weapon trafficking. In Latin America there is also enhanced human trafficking and child exploitation.

Australia and New Zealand

These countries are in a similar situation and maintain a similar policy to Europe.

TIMELINE OF EVENTS

Date	Event
1946	Creation of INTERPOL
1957	Introduction of the term “artificial intelligence”
1960s	Invention of the ARPANET
1991	Invention of the WWW
1997	Creation of UNODC
1999	Creation of EUROPOL
2001	Creation of the Convention on Cybercrime
2005	Creation of the VFAC

POSSIBLE SOLUTIONS

Cyber Security

The offences listed in the Historical Background section are the main issues you should propose solutions to. Most of them are very extensive and are committed via a lot of means, however, you should solely focus on how cyber security can be improved and be put to practice more effectively in order to eliminate them. One good strategy in writing your resolution would be to find out which of these crimes are more common in your country and mainly propose solutions to them. This will help you both in your research and during lobbying in the conference.

Some demonstrative issues that should be addressed are:

1. The existing organizations that deal with cybercrime. The organizations mentioned in this study guide, such as INTERPOL, VFAC etc., that cooperate with the UN, and the UNODC can contribute significantly in research in cybercrime and provision of expertise personnel. Therefore, mentioning them in your clauses and calling upon their assistance, would make your suggestions realistic.

2. Child sexual exploitation and abuse. Suggesting the usage of technology for the detection of online sex offenders and trafficking networks.

3. Safety of the public. Anything that can be done to help eliminate hacking and personal data theft. One way to achieve this would be the establishment of internet platforms in which users could report cases of cybercrime.

4. Internet censorship. Based on your delegation's policy you would either be in favor of or against censoring parts of the internet in order to achieve cyber security. This is a greater question of the amount of control the member states' governments shall have on the flow of information and what should be done in order to prevent access to websites of malicious content.

5. Anonymity in the web. There should be proposed measures for the prevention of anonymity, as well as measures for the detection of anonymous cyber criminals.

6. Financial cybercrime. Measures for the protection of online transaction from malware attacks.

Artificial Intelligence& Human Networks

The key aspects here are cooperation and transparency, meaning that all member states should work together and share information regarding developments in AI and human networks. Referring to their advantages, you should propose their usage for the benefit of the international community. It is, of course, also significant that you come up with solutions for the prediction and elimination of the problems that may occur with their usage.

BIBLIOGRAPHY

- "Cybercrime." Cybercrime / Cybercrime / Crime Areas / Internet / Home - INTERPOL, www.interpol.int/Crime-areas/Cybercrime/Cybercrime

- "Social Engineering Fraud." Social Engineering Fraud / Financial Crime / Crime Areas / Internet / Home - INTERPOL, www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud

- "Money Laundering." Money Laundering / Financial Crime / Crime Areas / Internet / Home - INTERPOL, www.interpol.int/Crime-areas/Financial-crime/Money-laundering
- "The Threats." The Threats / Cybercrime / Crime Areas / Internet / Home - INTERPOL, www.interpol.int/Crime-areas/Cybercrime/The-threats
- "Social Engineering Fraud." Social Engineering Fraud / Financial Crime / Crime Areas / Internet / Home - INTERPOL, www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud
- "Cyber Crime." FBI, FBI, 22 Mar. 2017, www.fbi.gov/investigate/cyber
- "What Is Sextortion?" FBI, FBI, 7 July 2015, www.fbi.gov/video-repository/newss-what-is-sextortion/view
- "Money Laundering Methods, Trends and Typologies." U.S. Department of State, U.S. Department of State, www.state.gov/j/inl/rls/nrcrpt/2003/vol2/html/29910.htm
- "Trafficking in Human Beings." Migration and Home Affairs - European Commission, 6 Dec. 2016, ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/trafficking-in-human-beings_en
- "Tips and Advice to Prevent Identity Theft Happening to You." Europol, 16 Nov. 2016, www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/tips-and-advice-to-prevent-identity-theft-happening-to-you
- "Conventions." Council of Europe, Council of Europe, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
- "Cybercrime." Europol, www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime.
- United Nations Office on Drugs and Crime." Introduction to Money-Laundering, www.unodc.org/unodc/en/money-laundering/introduction.html
- "United Nations Office on Drugs and Crime." Global Programme on Cybercrime, www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html
- "United Nations Office on Drugs and Crime." What Is Human Trafficking?, www.unodc.org/unodc/en/human-trafficking/what-is-human-trafficking.html
- Dennis, Michael Aaron. "Cybercrime." Encyclopædia Britannica, Encyclopædia Britannica, Inc., 27 Dec. 2017, www.britannica.com/topic/cybercrime

- The Editors of Encyclopædia Britannica. "Digital Rights Management." Encyclopædia Britannica, Encyclopædia Britannica, Inc., 25 Sept. 2013, www.britannica.com/topic/digital-rights-management
- Hosch, William L. "Piracy." Encyclopædia Britannica, Encyclopædia Britannica, Inc., 2 May 2014, www.britannica.com/topic/piracy-copyright-crime
- "Artificial Intelligence Meaning in the Cambridge English Dictionary." Cambridge Dictionary, dictionary.cambridge.org/dictionary/english/artificial-intelligence
- "The Business of Artificial Intelligence." Harvard Business Review, 7 Aug. 2017, hbr.org/cover-story/2017/07/the-business-of-artificial-intelligence
- Nogrady, Bianca. "Future - The Real Risks of Artificial Intelligence." BBC, BBC, 10 Nov. 2016, www.bbc.com/future/story/20161110-the-real-risks-of-artificial-intelligence
- "UN Artificial Intelligence Summit Aims to Tackle Poverty, Humanity's 'Grand Challenges'." UN News Center, United Nations, 7 June 2017, www.un.org/apps/news/story.asp?NewsID=56922#.WlU7lahl_IX
- Human Networks, www.pagebox.net/networks.html
- History.com Staff. "The Invention of the Internet." History.com, A&E Television Networks, 2010, www.history.com/topics/inventions/invention-of-the-internet
- "Internet Users by Country (2016)." Internet Users by Country (2016) - Internet Live Stats, www.internetlivestats.com/internet-users-by-country/
- Nspcc. "Child Sexual Exploitation." NSPCC, www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/child-sexual-exploitation/
- Nspcc. "Facts and Statistics." NSPCC, www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/child-sexual-exploitation/child-sexual-exploitation-facts-and-statistics/
- VFAC The Virtual Forum Against Cybercrime,no www.cybercrimeforum.org/index.jsp
- Agora International Journal of Juridical Sciences, univagora.ro/jour/index.php/aijjs/index
- Counterfeits on the Web a Growing Problem." IACC - International AntiCounterfeiting Coalition, www.iacc.org/online-initiatives/about
- "United States Institute of Peace." United States Institute of Peace, www.usip.org/