Committee: Security Council

Topic: The question of targeting cybercrime and the dark web.

Committee:	Security Council
Issue:	The question of targeting cybercrime and the dark web.
Written by:	Costanza Desiata
Position:	Chair

Introduction

The Internet is a networking infrastructure. It connects computers together globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet, therefore the primary purpose of the internet is to facilitate the population's sharing of information. The variety of associations one can have amongst the millions of computers in the internet can be a benefit as well as a drawback, users can exploit and sabotage the system for their own personal needs, in defiance of the fact that it is illegal. In the present circumstances, nearly 3 billion people (40%) have access to the Internet. The endless possibilities along with the vast amount of users have made the Internet a perfect place for cybercrime.

The internet is fundamentally made up of three different layers, these are: the surface web, the deep web and the dark web. The top layer, acknowledged as the

surface web, encompasses web pages that are visible when using search engines like Google. The deep web are web pages which search engines can't retrieve, and are therefore hidden, accessed via passwords and authorisation. For instance, any time an individual logs into an account he/she is accessing deep web content that won't show up on a search engine. The dark web is where cybercrime and cyber warfare transpire; it is a network of untraceable online activity and websites on the internet. They cannot be found using search engines and to access them you need to use specific software, configurations or have authorisation. They are used by lots of different people to keep their web activity hidden.

The United Nations clarifies two aspects of cyber Attacks: the political and military aspect known as cyber Warfare; the economic aspect known as cybercrime. Access to the Internet needs to controlled and restrained in order to make it a more secure setting, while protecting rights to information and controlling the risks of cybercrime and cyber Warfare. Access to the Internet needs to be controlled, so as to make it a more secure and safe network for information, while protecting rights to information and controlling the risks of Cybercrime and Cyber Warfare. In order to achieve this, several measures must be taken by the United Nations with respect to cyber security.

Definition of Key Terms

Dark Web

The dark web, also referred to as the darknet, is defined as an encrypted fraction of the internet that is not indexed by search engines.

Deep Web

The deep Web, sometimes called the invisible Web, is the large part of the Internet that is inaccessible to conventional search engines.

Cybercrime

Crime in which a computer is the gadget that, as a matter of fact, commits the crime. These crimes include: hacking, phishing, or spamming. Additionally, in cybercrime a computer is also used as a tool to commit an offense, such as child pornography or hate crimes.

Cyber Warfare

Politically motivated attacks that may destroy data or even cause physical damage to infrastructure of a specific country

The Internet

A global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to link several billion devices worldwide.

Digital Age

An era of human history based on information computerization. It is associated with the Digital Revolution, which refers to the growing number of people connected online in the world.

Cybercriminals

Entities that may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malevolent purposes.

The World Wide Web

A platform for online communications through the Internet, allowing people to share and access information from all over the world.

Denial-of-Service Attack

A security event that occurs when an attacker takeaction that prevents legitimate users from accessing targeted computer systems, devices or other network resources.

Cyber Space

The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries

Hackers

Criminals who perform cybercrime.

Darknet Markets

A darknet market is any market on the dark web meant for illegal purposes. To access a darknet market a user needs to use software, such as The Onion Routing (TOR) or The Invisible Internet Project (I2P)

General Overview

Cyber attackers have many advantages in carrying out their illegal activity without any form of impediment, for example: the law enforcement and jurisdiction finds it difficult to locate where cyber attacks take place. Therefore, it is by no means clear who the cybercriminals are, meaning that they can't be easily identified. Furthermore, it is financially uncomplicated to engage in activity within the cyberspace, consequently one can master its tools and use it against the state.

In the past cyber crime was committed mainly by individuals or small groups. Today we see highly complex cybercriminal networks bringing together individuals from across the globe to perpetrate crimes on an unprecedented scale. Cybercrimes can be more harmful than traditional ones, since cyber offenders can situate multiple attacks at any time, from anywhere, anonymously against information systems. Besides, since organizations become aware of unlawful use of electronic devices through information systems and electronic monitoring, a well-developed cyber-attack can cover its own traces. Cybercrimes can also damage critical infrastructure and other hardware structures.

Criminal organizations turning to the internet to facilitate their activities and maximize their profit in minimal time. These crimes aren't necessarily new, such as theft, fraud, illegal gambling, scale of fake medicines which can be labelled as darknet markets. These are evolving with the increase of opportunities presented before them. Commercial service is also a key aspect of cybercrime, it essentially means the exchange of goods. However, in the Dark Web, the goods mentioned are illicit. The bitcoin currency used for these transactions doesn't require the government's or bank's approval, instead, there are "miners" (a network of users) which control and verify these transactions. Therefore, bitcoin is a service that

serves practical purposes in enabling the Dark Web to be usable as they are uninsured and very difficult to track back to the person who spent them. Whenever a bitcoin transaction transpires, only the wallet ID is recorded, not the names of the buyers and the sellers. This emphasises the anonymity of cybercrime.

Additionally, another enabling mechanism of cybercrime is the Hidden Wiki, this site contains a catalogue of all the Dark Web Sites that are currently operating, user feedbacks on those sites, and information about what can be accessed through each site.

Pedophilia on the dark web works like a darknet market too. Similar to a drug darknet market, pedophile pictures can be bought in exchange for bitcoins. However, the Dark Web also offers publishing and discussion forums for pedophiles. There are two types of pedophiles on the dark web: a division contribute to this illegal activity by using its content, but are not active outside of the web, and others, who are active in finding new ways to live their sexual attraction. The Onion Routing Project (TOR) is a free software first created by the US Naval Research Laboratory. It does not provide anonymity in itself, but it allows the exchange of information between two different entities to be anonymous. It is crucial to know that TOR is the key to the Dark Web. One use of TOR is that It helps journalists get in contact with whistleblowers or victims that prefer their identity to be anonymous. It also allows people working for NGO’s to work without being traced.

Debates on cybercrime are created to try and compromise the usage of The World Wide Web, more so to try to demote and eradicate unsafe and illegal activity in the cyberspace. However, there is a “freedom” factor that should be taken into consideration. The internet shouldn’t be entirely restricted as users necessitate freedom of expression, along with having their personal information protected. Balancing the two requirements can come across as unattainable, also due to the fact that cybercrime has become a recently developed way to obtain money as

cybercrime schemes remain inexpensive and accessible to anyone with criminal intent.

Major Parties Involved

European Commission

The European Commission established a Communication on a European Cybercrime Centre in 2012 which has four main aims: 1. Serve as the European cybercrime information focal point; 2. Pool European cybercrime expertise to support Member States; 3. Provide support to Member States' cybercrime investigations; 4. Become the collective voice of European cybercrime investigators across law enforcement and the judiciary

The Onion Routing (TOR)

A software that creates a connection between several computers at a time that facilitates to hide an encryption. That implies that the start and end point of information traveling through the dark web remains unknown. The Onion Routing can be used for illegal purposes such as darknet markets, but also enables the right to anonymity.

International Criminal Police Organisation (Interpol)

The International Criminal Police Organization, more commonly known as Interpol, is the international organization that facilitates international police cooperation. As an international law-enforcement organization with 184 members, Interpol started to tackle computer crime very early, coordinating law-enforcement agencies and legislations, in regard to which Interpol made efforts to improve counter-cybercrime capacity at the international level.

The Asia-Pacific Economic Cooperation (APEC)

In the Asia-Pacific region, the APEC coordinates its 21 member economies to promote cybersecurity and to tackle the risks brought about by cybercrime.

Internet Corporation for Assigned Names and Numbers

The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization responsible for the IP-addresses on the Internet. ICANN is responsible for the assignment, country code and server management functions. This gives ICANN full control over the Domain Name System (DNS), which basically controls content representation on the Internet. As ICANN is incorporated under the US law it is criticized for acting as the mean for the US to control the web. However, the existence of the Regional Internet Registries (RIR) controlling ICANN as well as the seven keys around the world given to online security experts ensure that ICANN does not abuse its power.

The National Crime Agency (NCA)

The National Crime Agency is a national law enforcement agency in the United Kingdom. It was established in 2013 as a non-ministerial government department, replacing the Serious Organised Crime Agency and absorbing the formerly separate Child Exploitation and Online Protection Centre as one of its commands.

Global Cybersecurity Index (GCI)

Multi-stakeholder initiative to measure the commitment of countries to cybersecurity. Each country's level of development will therefore be analysed taking into consideration five categories: legal measures, technical measures, organizational measures, capacity building and cooperation. Cybersecurity has a large scope of application that spreads across many industries and sectors. It is a survey that measures the commitment of member states in order to raise awareness.

Global Commission on Internet Governance

The Global Commission on Internet Governance (GCIG) provides recommendations and practical advice on the future of the Internet. Its primary objective was the creation of "One Internet" that is protected, accessible to all and trusted by everyone. In their last report the Commission finalised courses of action that everyone needs to take to attain a more open and secure internet.

United States of America (USA)

The power that countries have over the Internet is crucial as cyber-governance links directly to cybersecurity and cybercrime. According to the Global Cybersecurity Index the USA is best prepared for any eventuality regarding a Cyberattack. The USA not only has the power to defend itself against cybercrime, but also the power it had to control the Internet in the past through ICANN (previously mentioned). Pressure from the international community led a slow separation between USA and ICANN assured by the "Affirmation Commitments" in 2009. However, in 2013 Snowden's revelations about NSA surveillance over the Internet contradicted these documents. Shortly after that, the US government announced that it would give up state control of ICANN.

Malaysia

According to the ITU Malaysia ranked third in the Global Cybersecurity Index 2014. This makes her a leading country in the cybersecurity field of Asia-Pacific. However, the country faced various incidents of attacks during the previous years. With the aim of fighting cyber-attacks the Malaysian governments supported in its 2016 agenda the improvement of cyber security measures through regional cooperation as well as collaboration between governments and various agencies.

The International Telecommunication Union (ITU)

The ITU is the United Nations specialized agency for information and communication technologies. ITU takes a human rights approach on the issue of cyber-security. Its vision and aim is to connect all citizens around the world through the World Wide Web. Hereby they fight for the right of access to the Internet. According to ITU's statistics Europe, North America (USA and Canada), Brazil and the Commonwealth nations are most committed to cyber-security. Furthermore, ITU provides guidelines and information related to cyber security.

Timeline of Key Events

Attacks increasing from the 1960s onwards led countries to

Date	Description of Event
1960	First occasion of "hacking" took place, led by students in universities.

1982	First three viruses that are able to attack Apple computers were invented, these made computers crash or leak information.
1985	First virus created that attacks PCs
1994	
1998	Concern about internet security triggers American computer services company called Netscape to develop Secure Socket Layer encryption for the safety of online transactions.
	First resolution was proposed to the UN, which was submitted by the Russian Federation/ First WSIS (World Summit on the Information Society)
23 November 2001	Convention of Budapest of the European Council took place. The treaty elaborated during the Convention was the first international treaty to address computer crime, specifically referring to security of computer networks, copyright violations, computer fraud and child pornography.
2002	Creation of TOR
2004	Adoption of the Budapest Convention on Cybercime.
2008	
2009	Proposal for an international Cybercrime Convention from several member states
April 2010	Chinese Google hacked into
	Proposal for a global treaty on cybercrime rejected due to the lack of progress between LEDCs and MEDCs

14th September 2011	
December 2011	Russia and China propose suggest an International Code of Conduct for Information Security
June 2013	
May 2017	ECOSOC conference on cyber security and development
	NSA (National Security Agency) information is leaked
	WannaCry Ransomware cryptoworm
	Petya (malware) global cyberattack
March 2016	

Previous Attempts to Resolve the Issue

- ➔ The world Summit on the Information Society (WSIS) was a conference held, sponsored by the United Nations, which covered the topics of : information, communication and in information society. One of its objectives was to unite the global digital divide separating rich countries from poor countries by extending internet access to LEDCs. In fact, this society formulated a resolution on the 12 December 2003 in Geneva which targeted cybercrime and the dark web.

- ➔ One of the largest and most infamous Dark Web marketplaces was Silk road. It was created in 2011 by Ross William Ulbricht , he obtained $13 million from allowing vendors to use his Silk Road Platform. The platforms not only sold drugs, but anything and everything that vendors put online. In October 2013, FBI discovered who was under Silk Road and finally shut it down. They concluded that over $1.2 billion sales had occurred which entailed 150,000

customers and 4000 vendors. This crisis depicts that illegal trade is a gargantuan business on the Dark Web.

- ➔ The United Nations Office on Drugs and Crime (UNODC) has worked in more than 50 countries to provide the necessary training, to sharpen investigative skills, trace cryptocurrencies as part of financial investigations, and use software to detect online abuse materialise and go after predators. As a result of this, a high-risk paedophile which had around 80 victims was arrested, tried and convicted. The training is carried out in partnership with the International Centre for Missing and Exploited Children and Facebook. This training is mainly focused in Central America, Eastern Africa and South-East Asia.
- ➔ Also, the UN has launched child sexual abuse reporting portals working with the Internet Watch Foundation, so that citizens can report images to prevent online exploitation

Possible Solutions

An assortment of solutions have already been applied, but unfortunately have had small-scale results which don't amount to the complexity of the situation. Technology improves daily, this is a major advantage as well as a struggle in terms of constantly having to ameliorate the international law to keep up with technological progress. The Dark Web is a brand new topic for a lot of policy-makers, therefore it is crucial that they become informed of all the aspects revolving around the dangers, as well as the benefits of it before enacting policies. Anonymity and lack of identity are also a significant issue with the users of TOR, as it is impossible to distinguish between innocent users and criminals while using this software.

A distinct line should be drawn between privacy and cybersecurity which would lead to delegates arguing the extent to which cybersecurity should be implemented to surveil individuals, as well as solving the issue of ICANN by proposing a way of guaranteeing an unbiased control of the internet.

Bibliography

"FBI Hosted Images of Child Sexual Abuse on Dark Web to Hack Pedophiles around theWorld." The Next Web RSS 24 Jan. 2016. Web. 10 July 2016. https://thenextweb.com/insider/2016/01/24/fbi-hosted-images-of-child-sexual-abuse-on-dark-web-to-hack-pedophiles-around-the-world/

"Pedophiles Seem to Make Up a Huge Chunk of Anonymized Web Traffic." Smithsonian. 10 July 2016. https://www.smithsonianmag.com/smart-news/pedophiles-seem-make-huge-chunk-anonymized-web-traffic-180953793/?no-ist

“International Communications Union.” World Summit on the Information Society. 12 December 2003 https://www.itu.int/net/wsis/index.html

“International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene”.Webology, Volume 4, Number 3, September, 2007. http://www.webology.org/2007/v4n3/a45.html

"GCI Charts & Tools." ITU Committed to Connecting the World. 11 July 2016. .https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2014_charts_and_tools.aspx

“Resolution adopted by the General Assembly” General Assembly. 27 April 2006 https://www.itu.int/net/wsis/docs/background/resolutions/60-252.pdf

“Legal and Political Measures to Address Cybercrime” Matheus M. Hoscheidt1 Elisa Felber Eichner. https://www.ufrgs.br/ufrgsmun/2014/files/WSI2.pdf

Global Commission on Internet Governance: “The Impact of the Dark Web on Internet Governance and Cybersecurity” Michael Chertoff and Tobby Simon. February 2015. https://ourinternet-files.s3.amazonaws.com/publications/GCIG_Paper_No6.pdf