1st International Model United Nations

Conference Leirion

Domotel Kastri Contemporary Hotel

October 29-31, 2021

Individual Freedoms in the Contemporary Era

Cybersecurity and Transnational Organized Crime

Security Council

George Laios, Leibniz University Hannover, Computer Engineering

Harald Rutsch, University of Twente, Technical Computer Science

Eve Vazaiou, Arsakeio Ekalis High School

Secretariat Guidance: **Fay Anagnostopoulou**, University of Athens

Academic Supervision: **Hendrik Schopmans**, PhD Researcher in Political Science at the WZB Berlin Social Science Center and the Free University Berlin

under the auspices of the

HELLENIC REPUBLIC

Ministry of Digital Governance

Leirion Alternative Library – Art Place

Contents

Introduction

It is undeniable that technology plays a key part in our daily lives. With the rise of the Internet of Things (IoT), the number of connected devices is only bound to increase. From automating tasks for us to enabling us to store and access data from everywhere via online data clouds, technology has a broad range of applications: It is used to help us communicate with the people we care about across the world, manage databases and even perform remote surgical operations with extreme precision. This is not limited to private individuals; companies are progressively deploying equipment connected to the Internet. Governments have also started to implement digital technologies to better perform their duties. Utilities have increasingly become digitalized, and computer controlled. Our world as we know it exists only because of computer systems and the Internet.

The benefits of computer systems are far reaching and immense ‘our society. Instant messaging and video sharing have become the norm, certain dangerous tasks no longer must be done by a human, machinery can be remotely managed and maintained, resources can be used more efficiently, this list can be expanded to a remarkably high degree.

Yet despite its undeniable charm, many dangers lurk among the advantages that technology has to offer. Technology aids us, but also condemns us to being constantly susceptible to “unseen” attacks.

There are many who would seek to exploit technology for their own, often criminal purposes. As such, cybercrime is evolving at an alarming rate, and it is up to us to introduce cybersecurity measures to counter it. Critical Infrastructure such as power grids, power plants, water services, hospitals, and gas pipelines are notorious examples of infrastructure that can be disabled or even sabotaged to harm the population and the government. Large enterprises such as Amazon or Google are also prime targets for such attacks.

Cybercrime is, however, mostly transnational, meaning that it might take place across different countries. For example, the attacker could be in a different country than the victim of the attack and they may have even used several computers in other countries as intermediaries (proxies) to reach their target and complete the attack. Therefore, cybercrime has proven quite difficult to combat, while its reach is immense, often affecting many people worldwide. Cybercriminals also adapt and find new methods to commit their crimes much quicker than cybersecurity forces are able to respond to these new threats, which is also one of the reasons as to why cybercrime is rampant.

In this Study Guide, we will be examining cybercrime in more detail, delving into its many guises and implementation methods and reviewing notable examples thereof. Major attempts to resolve the issue will also be discussed, along with possible solutions for the issue.

Interest in Knowledge

Back in the 1970s when computers and the Internet as we know it were still under development, security was easily identifiable. The Networks were limited in size and purpose and so was access. Most of the danger originated from inside the organization, meaning that in a case in which the network was breached it was only a matter of identifying who had access to the system and when the incident occurred.

In 1971, a researcher working at BBN Technologies realized he could create a program that could move in a network of computers and leave behind a trail of text. The text read "I'M THE CREEPER: CATCH ME IF YOU CAN." This was the first computer worm and spawned Malware as we know it. The very first fine for a cybercrime was handed out to a university graduate student who wanted to determine the total number of machines connected to the Internet by counting the total number of connections; unfortunately, he made a mistake and almost brought the early internet to a standstill. This became known as the Morris Worm and was the first large-scale attack on the Internet.

Since 1988 the landscape surrounding the Internet has changed dramatically. Cybercrimes are usually committed to accomplish certain goals which can range from destruction of public property to corporate espionage. We will highlight a few recent cases.

Solar Sunrise was a systematic cyber-attack which compromised over 500 government and private computer systems running Sun Microsystems Solaris Operating system. It had infiltrated numerous defense systems. In the end two Californian University students pleaded guilty. However, the Department of Defense no classified Information had been leaked.

In 2012 the USA allegedly launched operation "Olympic Games" developed in cooperation with Israel's intelligence service. The piece of code later know by the IT-Community as Stuxnet was designed to sabotage Iran's nuclear program by increasing the rotation of Uranium-enriching centrifuges beyond a safe limit and disabling their alarms, leading to them being destroyed. This forced Iran to the negotiating table and ultimately lead to the Iran nuclear deal. While one of the most well-known cases of malware it proves to be a dilemma. If one believes the allegations that the USA is the perpetrator of this attack, this would count as cyber-warfare, which is a concept we will be examining further on. The reason why we included this example this to show the effects the digital world can have on use.

W32.DistTrack, also more commonly known as Shamoon, is a modular computer virus targeting the then recent 32- bit NT kernel of Microsoft Windows. The virus that struck in 2012 was target at Saudi Aramco and Ragas, leading to multiple weeks of production outages and leading to a large loss in profits for the respective companies. Infected Operating systems would be rendered useless, around 30.000 Windows based systems were rendered useless at Saudi Aramco. It represented the largest computer attack to that date.

2017 saw the rise of one of the largest Indiscriminate Ransomware attacks to date. WannaCry, allegedly designed by North Korean actors, crippled thousands of computers in over 150

Countries. It worked by attacking out-of-date Microsoft Operating systems or systems which were considered end of life (Such as Windows XP). The attack had devastating consequences through the world and further spread could only be prevented by the discovery of an Internet kill switch.

The 2014 Sony Pictures Entertainment hack is a notorious example of corporate espionage. A North Korean affiliated hack group identifying itself as “Guardians of Peace” leaked confidential data in order to prevent the airing of the Satire Film” The Interview”, featuring a plot to assassinate the North Korean dictator Kim Jong-Un. As a result, some US theatre chains did not want to screen the movie and the movie was released online; North Korea denied all responsibility.

2021 saw the Colonial Pipeline ransomware attack which disabled a large amount of the computerized equipment and caused a mass panic in some states. While the attack had no consequences to the direct gasoline supply, it encouraged some buyers to buy large quantities of fuel and in turn produced a shortage. The owner of the pipeline had to pay 4.4 million dollars’ worth of bitcoin, of which 2.2 could be recover by the authorities. These kinds of attacks on Infrastructure are severe threat to a nation.

Methodological and Theoretical Background

Definitions of Key Terms

Please note that the key terms in this section have been sorted based on **relevance** and **importance** and **not alphabetically**.

Malware

Malware is the term we use to refer to **mal**icious soft**ware** code. Malware can cause significant damage to a computer system and plays a key part in committing cybercrimes.

It should be noted at this point that even though the terms "computer virus" and "malware" are used almost interchangeably in colloquial speech, they are not exactly the same thing. Viruses are a subset of malware, and the term virus is only used to refer to programs that aim to spread themselves to other devices via several means, be that via e-mail attachments or USB devices, just like a real virus would attempt to do.

There are several different types of malware, so let us quickly review the most common ones:

Spyware[1]	Spyware is malware that attempts to spy and extract information from you, such as passwords for your bank accounts. The most common type of spyware are keyloggers[2], programs that secretly monitor what the user types on their keyboard and send it back to the attacker. As mentioned before, keyloggers are usually intended to steal passwords, either because the attacker wishes to access your accounts for themselves, or because they wish to sell them online to others who would be interested in doing so.
Trojans[3]	Malware that disguises itself as a legitimate program (hence the name, which stems from the Trojan Horse), and once installed, starts running its malicious code while still pretending to be a legitimate application.
Worms[4]	A type of computer virus that duplicates and installs itself on other computers on the same local network, thus quickly expanding its reach while performing malicious activity undetected.
Ransomware[5]	Malware that encrypts all files on the user's computer, then asks the user to pay a ransom to the developer of the malware to get access back. Usually, payment needs to be performed via cryptocurrency, and the criminal often makes it so that there is a time limit after which the files will be deleted, so that the victim is has to pay as soon as possible.

[1] https://www.malwarebytes.com/spyware
[2] https://www.malwarebytes.com/keylogger
[3] https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html
[4] https://www.vipre.com/resource/what-is-a-worm-virus/
[5] https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html

Rootkits[6]	Rootkits manage to conceal themselves extremely well, making them hard to detect. A rootkit allows a hacker to access your device without your knowledge or consent.

DDoS (Distributed Denial of Service) Attacks[7]

An attack that attempts to render a system or a service unusable for an extended period of time by flooding it with millions of superfluous (fake) requests, causing it to be unable to respond to other legitimate requests and thus crashing it. This is usually performed with the help of networks of infected devices called Bot-Nets, which can send such requests en masse.

Bot-Nets

Bot-Nets (Ro**bot Net**works) are networks of computers that an attacker has managed to infect with specific malware and can now remotely control without the user's knowledge to further their plans, while using them to also infect new machines to expand the bot network.

Bot-Nets are often used in cyberattacks because:

- they can help the perpetrator mask their true identity since they are using the Bot-Net's computers as a proxy (intermediary) device to commit their crime
- they can be utilized to send requests to systems en masse, which is very helpful for several types of attacks, such as DDoS attacks.

A notable malware used to "recruit" computer systems into Bot-Nets is the Mirai malware[8], which primarily targets Internet of Things (IoT) devices running Linux such as printers, IP cameras and other smart home devices and essentially "brainwashes" these devices into doing whatever the attacker wants them to.

Cryptocurrency[9]

Cryptocurrency is an extensive topic, worthy of a separate Study Guide, so we will be only covering the basics, seeing as most illegal exchanges on the Internet use cryptocurrency as a means of payment.

Cryptocurrency is a form of digital currency. It is usually completely decentralized, meaning that there is no authority that can exert power over it, such as a government. This also makes transactions using cryptocurrency much harder to trace, which is why many criminals opt for this kind of virtual currency. For the same reason, money laundering is much easier when using cryptocurrency.

The most widely used cryptocurrencies are Bitcoin and Ethereum.[10]

[6] https://www.avast.com/c-rootkit
[7] Cloudflare is one of the world's leading anti-DDoS cybersecurity companies: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
[8] https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/
[9] https://www.investopedia.com/terms/c/cryptocurrency.asp
[10] https://time.com/nextadvisor/investing/cryptocurrency/types-of-cryptocurrency/#cryptocurrencies

Encryption

Simply explained, encryption allows a message to be obfuscated so that only specific people (usually only the recipient and the sender) can understand its contents. To decrypt a message, one needs the encryption/decryption key, which is a chain of characters that give an algorithm instructions on how to restore the original message. Some encryption algorithms use the same key for both encryption and decryption, some use different keys.

There are several methods that can be used to encrypt messages, but explaining them all would be quite lengthy, so all you need to know as delegates is that an encrypted message can only be decrypted and read by someone in possession of the relevant key.

> "Hello" = "Khoor"
> "Hello" becomes "Khoor" using the Caesar Cipher with a shift value of 3

[11]

Artificial Intelligence (AI) and Machine Learning (ML)[12]

Artificial Intelligence, often abbreviated as AI, is the concept of machines simulating the human thought process to make meaningful and smart decisions when confronted with specific situations, even ones that they have never experienced before.

Machine Learning (ML) is a subclass of AI and is essentially a practical implementation thereof. As the name implies, Machine Learning gradually teaches the machine which action it should perform based on a Reward-Punishment system.

For example, an AI machine is tasked with playing a videogame which it has never even encountered before. The machine is only told how to control the on-screen character and the goal of the game and is left alone to experiment. The machine then proceeds to make the character run into some spikes on the ground and loses. It perceives this as negative feedback, meaning that its actions were incorrect and need to be adjusted. When this loop of events is performed multiple times, the AI essentially teaches itself how to play. It will understand that it has to jump to avoid the spikes, for example - Not because it actually understands what jumping is, but because it understands that it must not touch the spikes. When it does indeed manage to avoid the spikes, it perceives this as positive feedback, meaning that its actions were correct.

Keep in mind that this explanation was kept extremely simple to make the concept easier to understand – In reality, this would take a lot of time and attempts!

[11] This is just an example of basic encryption, you do not need to know how it works, but if you are interested in learning more about the Caesar Cipher, take a look at the relevant Wikipedia page

[12] https://www.northeastern.edu/graduate/blog/artificial-intelligence-vs-machine-learning-whats-the-difference/

An introduction to cybercrime

Cybercrime is a word that most of us have, without a doubt, encountered multiple times, either on the news, or on the Internet.

When we think of cybercrime, the first thing that comes to mind is computer malware: simply put, little pieces of program code injected into a computer's operating system by an individual with malicious intent, which can cause substantial problems and pose a major threat to the computer and its user.

But to say that cybercrime equals (exclusively) malware would be wrong. Cybercrime is quite a broad term, as it encompasses a multitude of different types of crime, yet all of them share a common denominator: They are performed with the aid of a computer.

The well-known cybersecurity company Kasperksy defines cybercrime as follows:

> "Cybercrime is criminal activity that targets or uses (or both) a computer, a computer network or a networked device."[13]

Let us examine this definition in-depth: One can observe that there are two major categories of cybercrime, at least in terms of how it is performed.

So, cybercrime is a (computer-aided) crime that targets another computer system, correct? In this case, the victim's computer is the target of the crime, and the fact that was targeted is the crime itself. The malware (viruses) example that was mentioned before would fall into this category. Another example would be hacking a website's server to access or even change its contents without permission. In both of these cases, the final target is another electronic system.

However, cybercrimes do not necessarily have to target another computer system. As a matter of fact, the definition highlights that cybercrime may also involve utilizing computers to perform another, not computer-related crime. For example, creating a website to distribute child pornography or sell illegal substances would fit in this category. In this case, computers are just the means to a different end, namely the distribution of illegal content. No computer is targeted. Instead, a computer is simply used to enable the rest of the criminal act to take place.

[13] https://www.kaspersky.com/resource-center/threats/what-is-cybercrime
This definition has been slightly adapted to better correlate with the Study Guide's contents

Why is cybercrime so difficult to combat?

During the many attempts to bring cybercrime under control, the term "**Cybersecurity**" was coined. Cybersecurity encompasses the measures and efforts performed in order to reduce and tackle cybercrime.

Tackling the issue of cybercrime is much more difficult than it seems, which in turn makes cybersecurity much harder to achieve. But one might ask themselves just why cybercrime has proven so difficult to rid ourselves of. Unfortunately, the answer to that is quite complicated. Let us review some of the obstacles that cybersecurity experts are constantly faced with.

- Cybercrime allows the crime to happen from practically anywhere in the world (unless direct physical access to a system is required), so it often is what we call a "transborder" crime, since the criminal and the victims could be in different countries at the time of the crime. This creates many issues when trying to solve the problem for the following reasons:

    - Every country has different legislation, which is problematic when attempting to persecute the attacker. Which legal system will be used? What if the country from which the attack originated does not consider this particular event a crime? The countries need to coordinate their legal efforts, which might prove difficult to do without a proper legal framework.

    - How will the police forces of the two countries effectively communicate and exchange evidence to track the perpetrator? Once again, very efficient communication is required, which is difficult to achieve. Furthermore, there might be jurisdiction issues due to the transborder nature of the crime that prevent the police force of one of the countries involved from performing their searches for the culprit.

    - A cybercrime might be state-sponsored, meaning that a certain country has secretly supported or sanctioned it for its own benefit. In such a case, it stands to reason that the involved state will attempt to conceal this fact, thus making the investigation much more difficult for other affected parties and countries. Cyber-warfare, which we will be examining later on, is an example of this.

- Cybercrime has the added benefit of making the crime significantly less traceable back to its perpetrator, thanks to the use of secure encryption algorithms or layered computer networks (such as TOR, which we will be examining later on in this Study Guide).

  Especially the second method is a major roadblock for cybersecurity forces: When one uses the internet, they need to communicate with several networks to achieve their goals. These little communications are what we call "network traffic", and each "message" that is transmitted via these networks leaves behind what one could describe as "breadcrumbs". Following the path of the network traffic can lead the police to the perpetrator of a crime. However, by obfuscating their own network traffic by using software such as TOR, criminals make it hard for the police to track their location and identity.

- Cybercriminals often utilize networks of infected computers to perform some of their crimes, which makes it even harder to track them and also gives them more power exponentially, since the infected machines can infect new ones. These networks are called "Bot-Nets" and will be discussed further on in the Study Guide.

- Technology constantly evolves, and with it, so does cybercrime. Criminals constantly try to find exploits in tech systems which they plan to abuse. At the same time, "defending" and hack-proofing these systems is much harder than it is to break them.

  Picture a burglar trying to break into your house. You have to make sure that every single potential entrance has been locked and secured to prevent them from entering, whereas the burglar only needs to find a solitary entry point that is unguarded or poorly secured, and they will have managed to breach your home despite your efforts.

  As such, it is evident that the battle fought by cybersecurity experts is asymmetrical and thus an unfair one, since the criminals have a clear advantage.

  - The rise of Artificial Intelligence (AI) and Machine Learning (ML) can also help cybercrime thrive. While its application in criminal activity might be a niche thing to do, AI has its uses there as well.

    The same concept about the asymmetrical nature of the "fight" applies here too, for the same reasons. It is much easier to train an AI "offensively", i.e. to aid in performing the criminal activity, than it is to train it "defensively". As such, AI favors criminals more than it does law enforcement, which could prove to be a problem in the long run.[14]

- The average user of a computer may not be particularly well-versed in the topic of computers and cybersecurity. As such, they may fall victim to malicious software much more easily (e.g. by opening suspicious e-mail attachments) and thus become the victims of cybercrime.

[14] https://cset.georgetown.edu/publication/automating-cyber-attacks/, Ben Buchanan, John Bansemer, Dakota Cary, Jack Lucas, and Micah Musser, "Automating Cyber Attacks," (Center for Security and Emerging Technology, November 2020) (https://doi.org/10.51593/2020CA002)

- Combatting cybercrime requires tracking and detaining cybercriminals. However, in order to achieve this, governments will have to employ online surveillance, which might not resonate well with the population. Many questions are raised: To which extent is the government tracking our online activities acceptable? Is giving up our digital privacy for the greater good acceptable, since it means that more cybercriminals get caught? These are moral concerns that need to be addressed.

The deep web and the dark web: Hidden parts of the Internet

Web crawling and web indexing

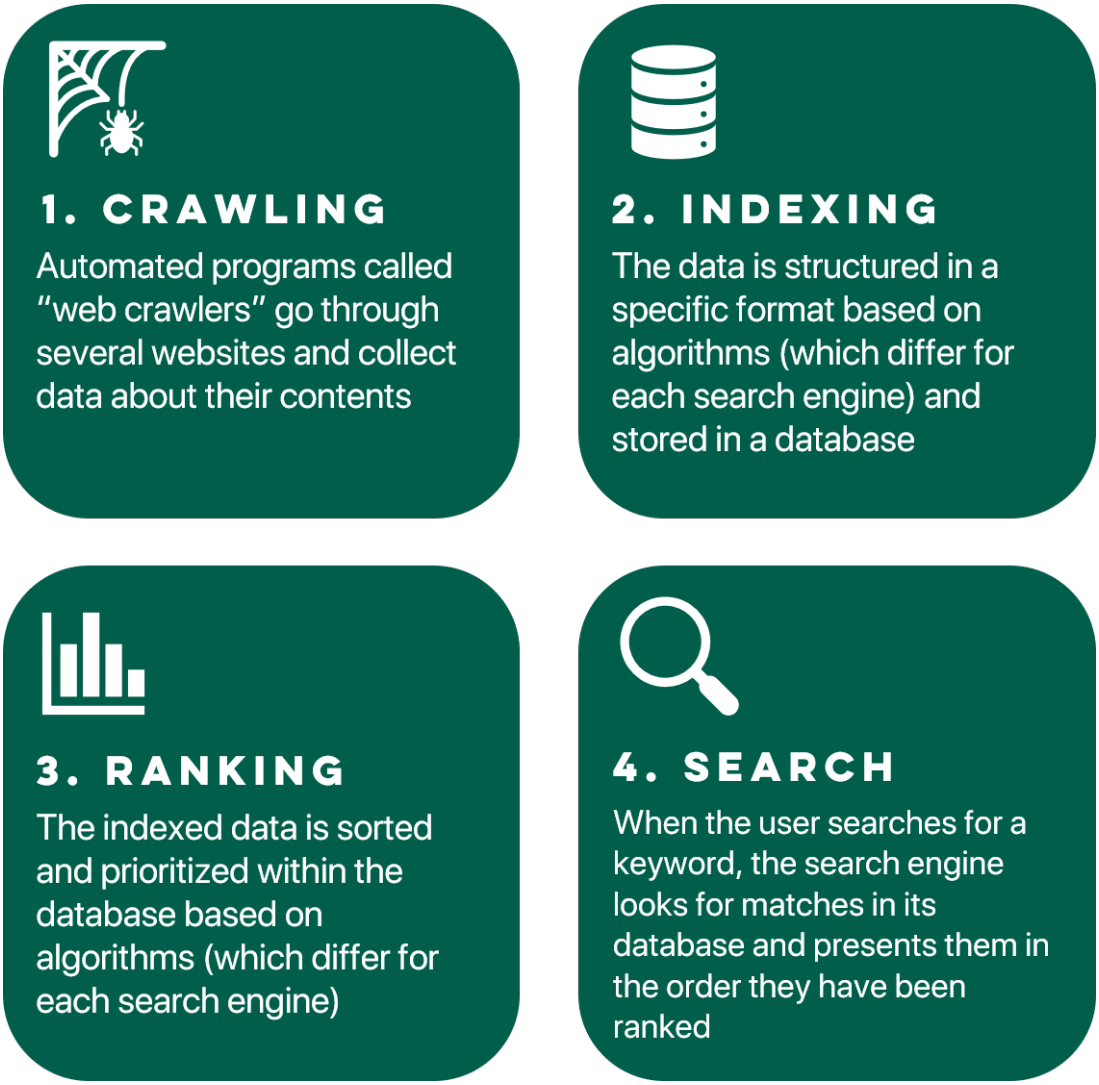
We've grown accustomed to using search engines for our treks on the Internet. They're simple to use, and help us find exactly what we're looking for in mere fragments of a second. All we have to do is input a keyword.

But how do these search engines work? The answer is web crawling and web page indexing. All search engines (Google, Bing, DuckDuckGo, Yahoo, just to name a few) utilize this technique to optimize their results.

Essentially, what happens is that these engines "crawl" through websites at regular intervals and collect unstructured data, such as a website's title and contents. That data is then organized and re-structured based on certain algorithms, which differ for each search engine. The final result is then stored in the engine's database and sorted among other results based on several algorithms. When a user performs a search, the database is searched for matches, which are then displayed to them. Once again, the sorting algorithms differ for each search engine, which is why two search engines might yield different results for the exact same keywords.

To speed up the web crawling process, search engines usually look for hyperlinks to other websites in every site they crawl through. If they find any, they move on to crawl through these newly discovered websites and so on.

Below you can find a simplified visualization of the web crawling and indexing process:



The surface web

The parts of the Internet that are visible and easily accessible via a search engine comprise the so-called "surface" part of the internet. However, not all websites are accessible in this way, which brings us to the next topic: The deep web.

The deep web

The deep web is a misunderstood part of the Internet, as it is often confused with the morally questionable dark web (or darknet), which we will be examining later on. **But these two terms are not the same.** While the dark web could be said to be a smaller part of the deep web, the latter is not necessarily dangerous and does not only include illegal content.

As a matter of fact, most of us have unknowingly used the deep web in one way or another.

Have you ever streamed a movie on Netflix, or made a payment via PayPal? Have you ever uploaded some private files to your Google Drive, OneDrive or Dropbox? Have you played an online game?

If you answered yes to any of these questions, chances are that you have used the deep web!

So, what exactly *is* the deep web? Unlike the surface web, there are certain parts of the internet that are not meant to be accessible by anyone, let alone by search engines. These include private databases or paid services, that an outsider should have no access to. These non-indexed and non-indexable websites are, pretty much, the deep web.

For example, your Google Drive folders are private, and hence not available as a result on Google! Search for them all you like, but you will not be able to discover them via any search engine. This is because they are part of the non-indexable web.

Netflix, Prime Video, or Hulu, also utilize the deep web. While they do have a main webpage that is accessible via a search engine, the repositories where the movies that you stream are stored are hidden and not indexable. In this case, this is done to protect the intellectual rights of said films and to prevent piracy.

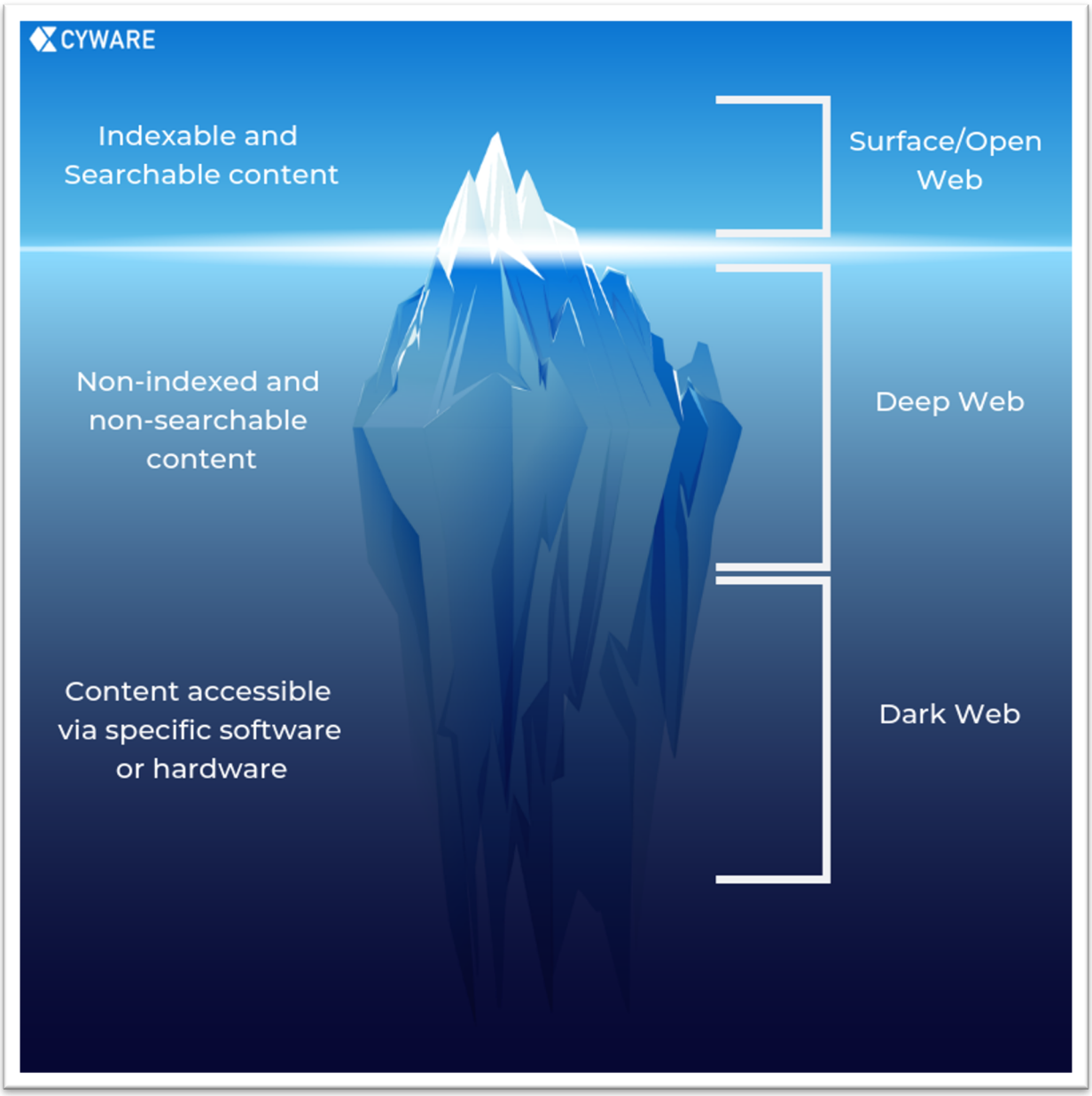
PayPal as well as other online banking services also use the deep web to protect the users' privacy and keep any financial records safe from outsiders.

Last, but not least, even certain online game services are inaccessible via normal search engines to make hacking and cheating much more difficult, and also because a player would have no legitimate reason to have direct access to these services.

Of course, the deep web may also include other types of content, such as content that has been censored in a specific region and is thus only accessible via dubious means on the deep web. However, the vast majority of the deep web's content is quite harmless.

What's shocking is that experts estimate the deep web to comprise about a staggering 90% of the entire Internet[15], thus much more than the visible part. You might have seen a similar picture before, but it makes for quite an accurate analogy:

(Source: https://cyware.com/educational-guides/cyber-threat-intelligence/how-is-surface-web-intelligence-different-from-dark-web-intelligence-393c)



[15] https://www.kaspersky.com/resource-center/threats/deep-web

The dark web[16]

The dark web, also referred to as the DarkNet, is technically a small part of the deep web. However, what makes it differ from the latter is the fact that on top of its content not being discoverable by normal means, users also need specific software or (in rare cases) hardware to access it. For example, one might need a specific browser, such as the onion browser TOR.

The dark web has many "gray areas". It offers much more privacy than the deep web due to it being even harder to access, so people who are being wrongfully persecuted or censored by an oppressive regime may resort to using it to voice their opinions.

While it is true that the dark web does not exclusively host indisputably illegal content and might only be used by some people simply because of the extreme privacy it offers, a non-negligible number of illegal activities take place in it exactly because of this enhanced anonymity. From selling weapons, drugs, and sensitive information to organizing networks of assassins for hire or people distributing child pornography, the darknet can be a haven for crime.

[16] https://www.investopedia.com/terms/d/dark-web.asp

TOR - Onion routing

TOR stands for "**T**he **O**nion **R**outer" and it is an open-source web browser [17]that uses onion routing to offer significant privacy and even access websites that would normally not be accessible by another browser.

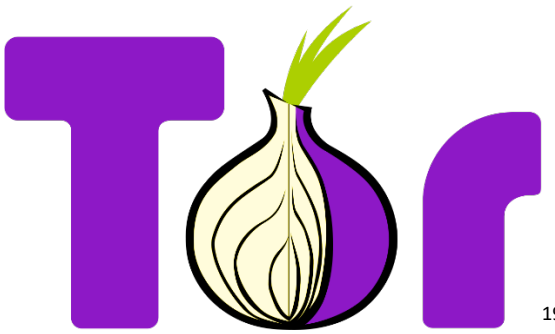
A prototype Onion Router was developed in 1995 by the U.S. Navy as a means of securing the Navy's online communications.[18]

Earlier, we mentioned network traffic and how it leaves digital "breadcrumbs" that can be traced back to a user. Onion routing essentially redirects the traffic coming from your computer at least three times between different volunteer computers across the globe called "TOR relays".

With each and every "bounce", the path of your network traffic becomes more and more obfuscated and harder to trace back to you, since technically, your computer does not directly connect with the server of the service you were trying to access, but it connects with TOR relay A, which in turn connects with TOR relay B, which then connects with TOR relay C and so on, until the final TOR relay directly connects to the target server.

TOR does **NOT** make you completely untraceable, it only makes it much harder for someone to do so.

Every time your traffic reaches a new TOR relay, we say that it has reached a new onion layer. Because of how TOR works, essentially creating several layers of computers between the user and the target, it is often compared to an onion, which has many layers. Hence the name ("The Onion Router") and the logo:


[19]

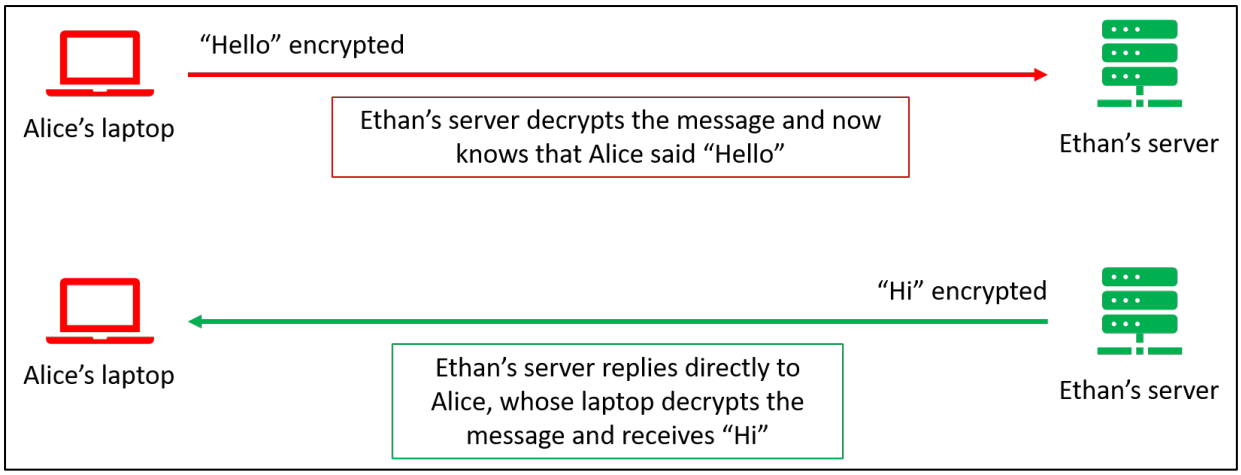
Certain links ending in ".onion" are the so-called "onion links", which point to hidden websites only accessible using TOR's infrastructure.

TOR is a concept that can prove to be quite confusing, so let us better visualize how it works.

[17] https://www.torproject.org/
[18] https://www.torproject.org/about/history/
[19] https://en.wikipedia.org/wiki/Tor_(network)#/media/File:Tor-logo-2011-flat.svg

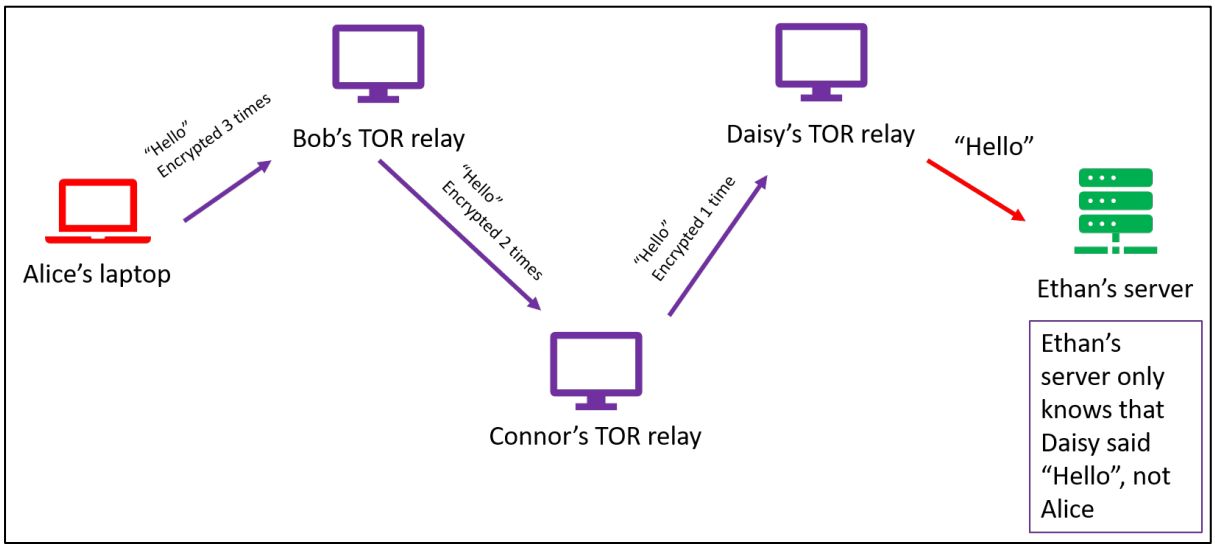
Suppose that Alice want's to access Ethan's server and say "Hello", to which Ethan's server should respond with "Hi".

Here's how this would work without TOR:
(Please note that the following images are a very simplified explanation and not 100% accurate. Their purpose is to better help you understand how TOR works in theory, so a lot of steps have been omitted)



As expected, Alice's laptop simply sends "Hello" to Ethan's server, and the latter responds with "Hello". Ethan's server knows that it was Alice who sent the message.

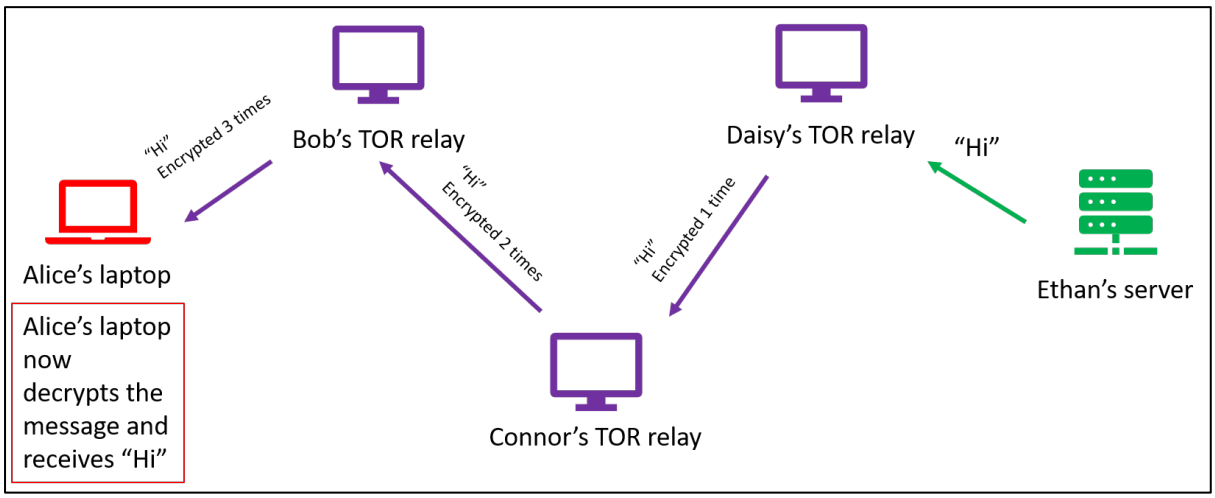
But what if Alice did not want Ethan to know that she is the one who sent the message? In this case, Alice could use an onion routing browser. Let's see what would happen then:



The message by Alice is encrypted as many times as it will be redirected via TOR relays. Every TOR relay only knows the encryption key of the previous TOR relay, so none of the relays (except for the last one) can completely decrypt the message on their own, since it has been encrypted multiple times and each relay can only remove a single layer of encryption. This

ensures that even if one of the TOR relays is leaking information, that information will still be encrypted and not understandable by anyone who comes across it.

With each bounce, the message loses one layer of encryption, until it reaches the final relay. Then, it is delivered to the target server. However, even though Alice sent "Hello", Ethan's server only knows that Daisy sent "Hello", not Alice. So, Ethan's server responds with "Hi" to Daisy. Let's see what happens now:



Daisy's relay now encrypts the message once and sends it back to Connor's relay, who also adds a new layer of encryption and sends it to Bob's relay. Finally, Bob's relay does the same and sends it back to Alice. Essentially, the reverse process is performed.

It should be noted that TOR makes sure that Alice has all the encryption keys, so she can remove all layers of encryption and read Ethan's reply: "Hi". Ethan however, **has no idea that Alice ever received this message, since he only sent it to Daisy, who he thought was the one who sent "Hello"**.

This was a simplified explanation on how an onion network functions. The important thing is that the server does not really know who initiated the request. Tracing the traffic back to Alice can be difficult, since many proxy computers are involved in between.

A significant downside to using TOR is that because of the many layers involved, browsing the Internet is noticeably slower.

The many forms of cybercrime

One would be surprised by how many diverse forms a cybercrime may take. Cybercrimes can have several ulterior goals, and criminals around the globe have been abusing the power of computers to perform them for completely different purposes over the years.

1. Cybercrime as a means of fraud

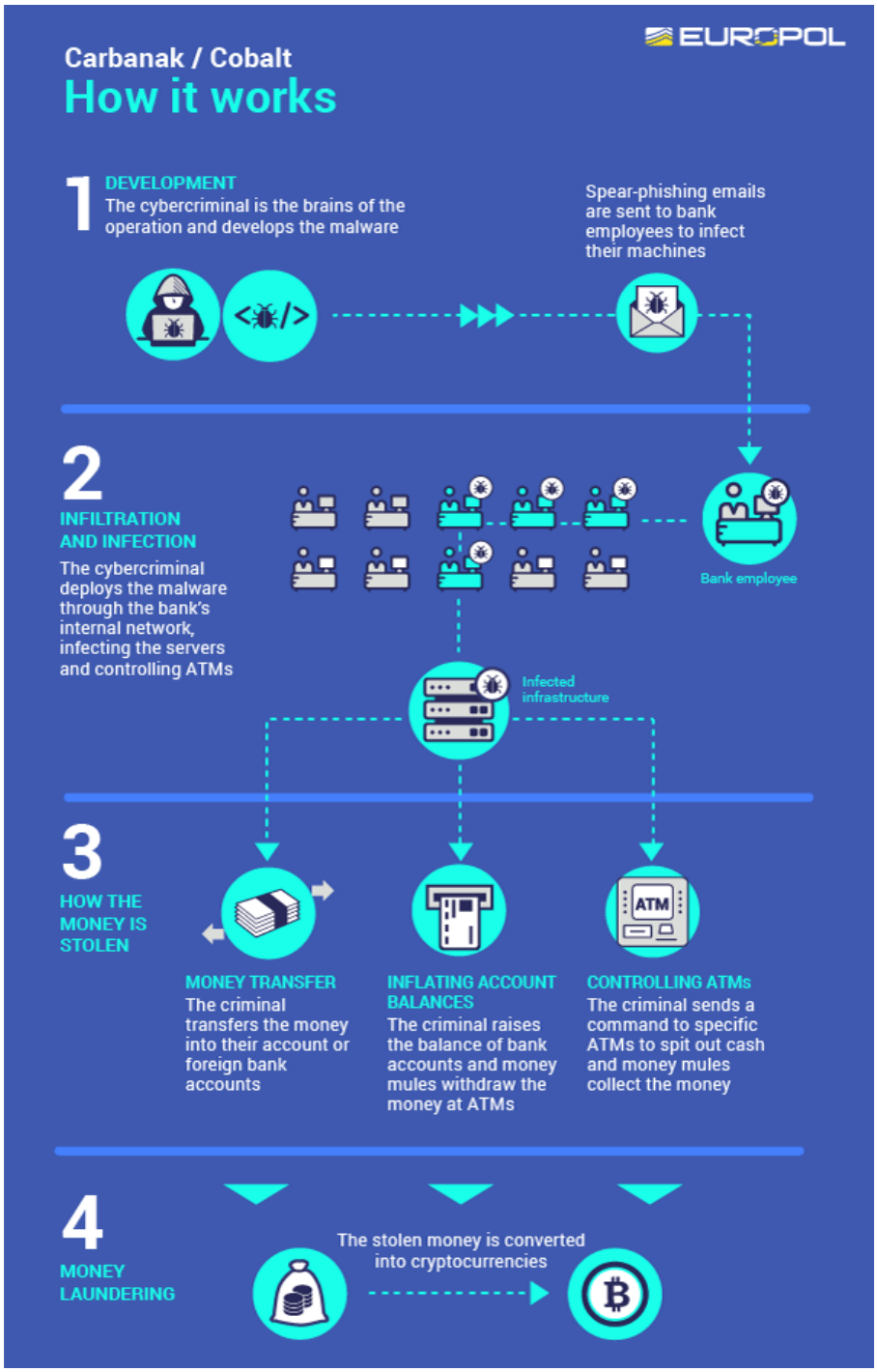
Aim	• Extracting money or information either by tricking the victim or hacking a system

Methods used and other notable information	• Usually takes the form of a scam to trick people into handing the criminal sensitive details or money (e.g. phishing, where a criminal creates a website that looks almost identical to the real version of a well-known website with the aim of tricking users into entering sensitive information on the fake website, which will be intercepted by the criminal)
	• Another form is hacking the database of organizations or companies (e.g. a bank or an insurance company) with the aim of extracting private information or compromising bank accounts to steal money from
	• Some criminals may infect computers with malware to achieve this:
	  ○ Key-loggers that track which keyboard buttons are pressed and send the data to the attacker, so that they can intercept sensitive data such as passwords
	  ○ Creating Bot-Nets to further their plans

Possible effects	• Monetary theft • Identity theft (the criminal can impersonate the victim online) • Breach of privacy
Notable examples	• The Carbanak/Cobalt malware Since 2013, a cybergang had been targeting over 100 financial institutions across the globe with the aim of stealing funds. It wouldn't be until 2018 that Europol would manage to apprehend the leader of the cybercriminals. According to Europol's press release[20], "the leader of the crime gang […] has been arrested in Alicante, Spain, after a complex investigation conducted by the Spanish National Police, with the support of Europol, the US FBI, the Romanian, Moldovan, Belarussian and Taiwanese

[20] https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain

authorities and private cyber security companies.". The criminal operation resulted in losses over a billion euros! Here is how the criminals ran their operation:



(Sources: https://www.europol.europa.eu/publications-documents/carbanak/cobalt-infographic, https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain)

2. Cybercrime as a means of disruption

Aim	• Disruption of a technical system, optionally with monetary benefit for the attacker

Methods used and other notable information	• Computer viruses, trojans, rootkits, worms, ransomware (explanations will be included) and other malware that damage computers
	  ○ Malware may often spread from computer to computer in a computer network, making it extremely hard to stop the infection once it has started
	  ○ Malware may often be difficult to detect, especially if the user is not tech-savvy
	  ○ In the case of ransomware, the attacker may demand money to restore access to an affected system, usually in cryptocurrency
	• DDoS (Distributed Denial of Service) Attacks can also be used
	• Some attackers may simply commit such a crime just to prove their ability to do so, with no benefit in mind
	• Many organizations may not have set up protection versus these kinds of attacks and may therefore be vulnerable

Possible effects	• Major disruptions of systems, financial losses • Serious damage if these systems regulate important aspects of a city's infrastructure (e.g. traffic lights system, railway system, water supply system, etc.), may cause injury or even the death of people
Notable examples	• The Dyn DDoS attack (2016)[21], a sequence of three DDoS attacks targeted at major service providers hosted by provider Dyn. It mostly affected users in North America and Europe and led to several services being unavailable for extended periods of time, including Netflix, Amazon, Twitter, Reddit, PlayStation Network, GitHub and even Spotify. It is believed that the attack was performed with the help of a Mirai-infected Bot-Net comprising several IoT devices, such as printers and smart home devices. • The GitHub DDoS attack (2018)[22], yet another DDoS attack that targeted GitHub and marked one of the first times that the "Memcached" attack method was used.

[21] https://www.ncta.com/chart/understanding-the-dyn-ddos-attack?share_redirect=%2Ftopics#colorbox=node-2825, https://www.gremlin.com/blog/after-the-retrospective-dyn-ddos/
[22] https://www.wired.com/story/github-ddos-memcached/

This is a very dangerous type of DDoS attack since it requires no Bot-Nets and has been known to be able to flood the target with extreme traffic (even up to a terabyte) by essentially sending negligible amounts of traffic and amplifying it by repeating the requests until it becomes quite substantial.
This is also the reason why no Bot-Nets are necessary for this kind of attack, since even little traffic can be amplified by the attacker to reach great sizes, whereas normally the attacker would need multiple systems sending requests simultaneously to achieve such traffic.
As a matter of fact, GitHub was hit with a whopping 1.3 Terabits per second worth of data for 15 to 20 minutes, which would make this one of the most significant DDoS attacks ever.

- The Melissa virus (1999)[23], which spread very quickly among computers by silently forwarding itself as an email attachment and tricking more users into thinking it was just a Word document. When opened, it would run macro commands on the system that allowed it to repeat the process, and so on. This virus caused email servers throughout the world to become overloaded, and while its creator did not intend to somehow benefit from it, the chaos it caused made it one of the most notable "early" viruses in computer history.

3. Cyber-terrorism and cyber-warfare[24]

Before we examine this section of the guide, it would be advisable to clearly explain what cyber-terrorism and cyber-warfare are and how exactly they differ from each other.

Cyber-terrorism, as the name implies, comprises using computers and technology to engage in terrorist activities, aiding in their organization and execution.

On the other hand, cyber-warfare is a less self-explanatory term. After all, no country has officially ever declared a cyber-war on another state! However, this does not mean that cyber-warfare is non-existent. On the contrary, it just might be more prevalent than ever nowadays, albeit much too difficult to detect on time.

So, what exactly does cyber-warfare entail and how is it different from cyber-terrorism? Simply put, cyber-warfare is what a war would look like if it took place completely virtually. You will see no weapons, no tanks and no front-line soldiers in such a fight. Instead, cyber-warfare aims at utilizing the technology of the attacking state to spy on and/or disrupt the

[23] https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519
[24] https://www.sciencedirect.com/topics/computer-science/moonlight-maze, https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm

target country and its technology and infrastructure. Usually, these attacks are state-sponsored, meaning that the attacking state will "outsource" them to a hacking group, so as to not be directly tied to the attacks. The state will secretly fund, support, and attempt to cover-up the hackers' misdeeds.

While it does sound similar to cyber-terrorism, keep in mind that they differ; the latter has the clear goal of causing damage, as the perpetrators are usually extremists who are motivated by their fundamentalist beliefs and thus specifically wish to harm their targets, whereas cyber-warfare is, as was mentioned before, state-sponsored and serves as a way of one state gaining an advantage over another. Thus, it is not uncommon for cyber-warfare to only restrict itself to espionage instead of directly attempting to harm infrastructure or humans.

Cyber-warfare can also be used to influence events in another country silently, a process referred to as a "foreign influence operation". An example of this could be manipulating the results of an election or even something as simple as attempting to sway public opinion by using bots to create fake social media accounts in the target country, which are then used to promote whatever message the attacker wants them to, often including misinformation.[25]

Aim	• Like cybercrime as a means of disruption, the goal is the disruption of a technical system, but this time with the aim to intentionally cause damage to a specific system or to humans depending on it (only in the case of terrorism). • It should be noted that, as mentioned in the relevant section above, cybercrime as a means of disruption can also cause harm to humans, but the difference between that case and terrorism is that in the former, said harm is not the main intention of the attack, whereas in the latter it may very well be the primary goal of the attacker.

Methods used and other notable information	• Cybercrime is used as a weapon, usually to disrupt critical infrastructure
	• Malware aimed at targeting disrupting such critical systems
	  ○ It spreads from system to system, using them as a means of transportation while otherwise remaining dormant and thus undetected
	  ○ Upon reaching the target system, it unleashes its attack
	• DDoS (Distributed Denial of Service) Attacks against critical infrastructure
	• Once again, many organizations may not be adequately prepared to defend themselves from such an attack or to preemptively prevent it

[25] https://www.fbi.gov/investigate/counterintelligence/foreign-influence, https://prevency.com/en/what-is-social-media-warfare/

Possible effects	• Major disruptions of systems, financial losses • Gaining an edge on a target (e.g. espionage in cyber-warfare) • Injuries and/or loss of human life in the case of terrorism
Notable examples	• Stuxnet (discovered in 2010)[26] **What was Stuxnet and how did it work?** At about only a meager 500 KB, one would not think that the worm known as Stuxnet could have such devastating effects. Stuxnet specifically targeted Programmable Logic Controllers (PLCs), hardware components used to automate industrial machines. The infection is believed to have started via the insertion of an infected USB-Stick into a computer. Stuxnet would then travel from infected Windows machines to other machines in the local network, infecting them in the process as well, while looking for specific Siemens-made SCADA (Supervisory Control and Data Acquisition) systems, which, simply put, are essentially industrial automated systems. Once it found a compatible Siemens SCADA system, it would then compromise its PLCs using a zero-day-exploit, which allowed Stuxnet to not only control parts of the infected system but to also spy on the its data on behalf of the worm's creators, all while masking its presence by relaying seemingly normal data back to the system's users. Stuxnet was the first worm to target SCADA systems. **What was Stuxnet used for?** The actual goal of the authors of Stuxnet is still a controversial topic, as most of it is speculation. However, given that the people who expressed these speculations were cybersecurity experts that closely analyzed Stuxnet, their opinions are of great interest.

[26] https://spectrum.ieee.org/the-real-story-of-stuxnet

Ralph Langner, a cybersecurity expert who helped analyze Stuxnet and who was the one to identify that it only targeted PLCs, was convinced that the malware was created by its authors with a very specific target in mind, given how it needs to be manually inserted into a computer network via a USB stick to begin the infection.

Ralph Langner

He also speculated that the target was the Iranian nuclear program. According to Langner, Stuxnet was meant to make the centrifuges spin out of control, thus breaking them, without the operators noticing until it was too late.[27]

Iran has confirmed that this was indeed a cyberattack against its uranium enrichment facilities, however it seems to have toned down the impact of the attack, seeing as its then-President Mahmoud Ahmadinejad stated that "[The perpetrators] succeeded in creating problems for a **limited** number of our centrifuges with the software they had installed in electronic parts […] Fortunately our experts discovered that and today they are not able [to do that] anymore".[28]

There is, however, evidence suggesting that the damage done was much greater than officially implied.

- In 2009, the head of Iran's Atomic Energy Organization (AEOI) resigned after 12 years, for unnamed reasons[29]. Many believe that this was because of the damage Stuxnet caused.
- The Institute for Science and International Security (ISIS), founded and ran by former UN International Atomic Energy Agency (IAEA) nuclear inspector David Albright, pointed out that about a thousand centrifuges that were affected between the late months of 2009 and January 2010 were decommissioned and that Iran was trying to conceal this fact by covertly replacing them with new centrifuges[30].

[27] https://www.langner.com/stuxnet/
[28] https://www.reuters.com/article/iran-ahmadinejad-computers-idAFLDE6AS1L120101129
[29] https://www.reuters.com/article/uk-iran-nuclear-resignation-sb/head-of-irans-atomic-energy-body-resigns-idUKTRE56F2CM20090716?edition-redirect=uk
[30] https://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

Who was behind Stuxnet?
The precision and complexity of the malware, as well as how effectively it was able to mask its existence both until and after it reached the target systems convinced many researchers that its creation must have been sponsored by a nation's government. In 2011, Langner speculated that Stuxnet was created by the United States in collaboration with the Israeli Mossad, a claim which still remains unconfirmed.[31]

- The Moonlight Maze Incident[32]
  Moonlight Maze is a well-known cyberespionage campaign which started in 1996 and was only discovered in 1999, a staggering three years later. Its long-term scope and the difficulty in detecting it earned this incident the status of a so-called "Advanced Persistent Threat" (APT).[33]
  Among others, the attack targeted several US government and military networks, including even NASA.

  When it was discovered, the public opinion linked it to Russia, but at the time, this could not be proven.

[31] https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyber_weapon
[32] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf, https://www.forbes.com/sites/jodywestby/2020/12/20/russia-has-carried-out-20-years-of-cyber-attacks-that-call-for-international-response/
[33] https://www.forbes.com/sites/jodywestby/2020/12/20/russia-has-carried-out-20-years-of-cyber-attacks-that-call-for-international-response/

The first article that mentioned "Moonlight Maze" appeared on 25 July 1999, The Sunday Times, London

THE SUNDAY TIMES · 25 JULY 1999

OPERATION MOONLIGHT MAZE

Missing secrets

Russian hackers steal US weapons secrets

by Matthew Campbell Washington

[34]

The perpetrators attempted to create backdoors in affected systems, which means that they were able to access the system remotely, without any permission whatsoever.

The culprits behind the attack remained unknown for quite some time, until two decades later, in 2017, four computer scientists from London's King College and cybersecurity firm Kaspersky Labs were able to trace a server used in the attack.[35]

[34] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf

[35] https://www.secureworld.io/industry-news/moonlight-maze-lives-on-researchers-find-link-to-current-apt, https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf

The four researchers
Thomas Rid, David Hedges, Daniel Moore, and Juan Andres Guerrero-Saade at King's College in London, March 2016

[36]

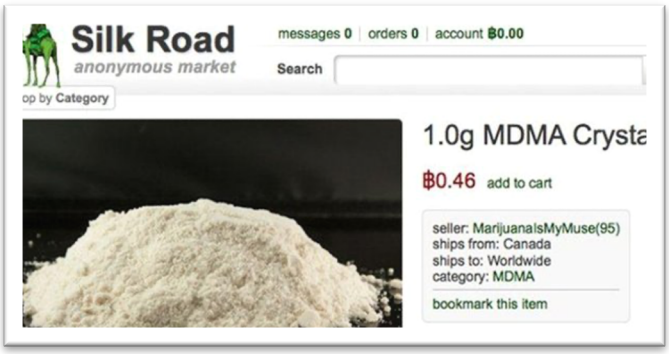
After researching their findings for a year, they were able to link the attack to a Russian-speaking hacking group called Turla, which suggests that Moonlight Maze was indeed an intelligence-gathering operation targeting the US which had been endorsed and state-sponsored by Russia.

[36] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf

Other illegal activities performed online

Cybercrime doesn't always have to involve malware and hackers. The dark web hosts several illegal services typically accessible only through onion networks. As has been mentioned before, cryptocurrencies (usually Bitcoin) are used for payment.

Illegal black markets



- Drug trafficking (e.g. SilkRoad)
- Illegal arms trade
- Sales of sensitive data (stolen passwords, credit card data, etc.) and malware
- Human trafficking & prostitution
- Organ trafficking
- Distribution of pornographic content involving minors (child pornography)
- Hacking groups (or individual hackers) performing cyberattacks on demand
- Contract killing (Assassins for hire)

Some notable examples include

- DarkMarket, which, according to Europol, was the world's "largest illegal dark web marketplace", with about half a million users.[37] (Not to be confused by a dark web market going by the same name, which was shut down in 2008).

It was shut down in 2021 by Europol and several other EU national cybersecurity and police forces, most notably those of Germany, who arrested an Australian national who they believe is the one running the market.

DarkMarket allowed users to purchase products such as stolen identities and credit card data, malware, SIM cards, and more.[38]

- SilkRoad[39], a dark web black market which was launched in 2011 and shut down 2013 with the help of the FBI. It was operated and accessed with the help of TOR networks. Its customers could buy several unethical products, most notably illegal narcotic substances, but also stolen data, such as passwords, etc. Its founder, Ross William Ulbricht (pictured on the right), is now serving a life sentence in prison.

The name SilkRoad references a historical trade route connecting the Western with the Eastern world in ancient times.[40]

[37] https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down
[38] https://www.dw.com/en/largest-illegal-darknet-marketplace-darkmarket-taken-offline/a-56200737
[39] https://www.investopedia.com/terms/s/silk-road.asp
[40] https://www.britannica.com/topic/Silk-Road-trade-route

- Boystown[41] was a darknet platform with approximately 400.000 international users, which focused on the sexual abuse of children and the distribution of audiovisual material thereof. Fortunately, the website was taken down in early 2021, and four German individuals were arrested - three in Germany and one in Paraguay.

- An hitmen-for-hire service was recently targeted by Europol, following the arrest of an Italian national who is suspected of having hired an assassin via the marketplace. The assassin is thought to have been found on a TOR network site, and to have been paid about 10.000 EUR to end the life of the man's former girlfriend. Luckily, Europol was able to prevent this from happening.[42]

- Wall Street Market was yet another large darknet marketplace similar to SilkRoad, which sold several products, ranging from drugs to stolen data and even malware. It was shut down by Europol, the FBI, and several other cybersecurity forces (notably those of Germany) in 2019. According to Europol, the site had more than 1.150.000 users and about 5.400 vendors![43]

- Silkkitie (also referred to as the Valhalla Marketplace) was a black marketplace on the dark web serving the same purpose as SilkRoad and Wall Street Market. It was shut down in 2019 by Europol and the Finnish authorities at about the same time as Wall Street Market (in a simultaneous operation).[44]

- Welcome To Video was a darknet site that operated on Bitcoin and promoted the distribution of child pornography. It was run by 23-year-old South Korean national Jong Woo Son. The site was taken down in 2018 and many children that were being abused by the members of the site were located and rescued.[45]

- The ShinyHunters hacking group is a group of hackers that steals passwords and then sells them on the dark web. Surprisingly, they have also published some of the content online for free, such as the data they managed to steal from a dating app with a focus on physical and mental well-being called "MeetMindful". The data was included in a 1.2 GB file containing personally identifiable information about the app's users which was made available for free on the dark web and was viewed by over 1.500 people.[46]

[41] https://www.europol.europa.eu/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-million-users
[42] https://www.europol.europa.eu/newsroom/news/dark-web-hitman-identified-through-crypto-analysis
[43] https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces
[44] https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces
[45] https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child, https://www.dw.com/en/hundreds-arrested-in-global-dark-web-child-pornography-investigation/a-50861673
[46] https://threatpost.com/meetmindful-daters-compromised-data-breach/163313/

- Lolita City was an onion network website where child pornography was being distributed. In 2011, it was targeted by the hacktivist group Anonymous (pictured on the left). The Anonymous are hackers who, according to themselves, put their skills to use for a good purpose. Anonymous managed to DDoS and temporarily shut down the website during what they called "Operation Darknet", which aimed to eradicate child pornography from the dark web.[47]

Terrorist groups

Many terrorist groups utilize the anonymity that the Internet can provide them with to organize terrorist attacks and/or recruit more people. These groups do not necessarily perform terrorist cyberattacks like the aforementioned ones, but they use the Internet to coordinate "physical" terror attacks. An example of such a group would be the United Cyber Caliphate (UCC)[48], an assembly of hackers allied with the Islamic State of Iraq and Syria (ISIS), also known as the Islamic State of Iraq and the Levant (ISIL).

[47] https://arstechnica.com/information-technology/2011/10/anonymous-takes-down-darknet-child-porn-site-on-tor-network/
[48] https://www.trackingterrorism.org/group/united-cyber-caliphate-ucc-islamic-state-isis

The legal system: preventing and combating cybercrime

> "Terrorists using the Internet for their purposes does not equal cyber-terrorism. However, by increasingly engaging in cyber-space, and given the availability of cyber-crime as a service, one can assume that they would be in the position to launch cyber attacks"
> ENISA Threat Landscape 2015

Since Cybercrime can be committed by offenders anywhere in the world with internet connection, the outcome of cyberattacks can be experienced outside of the country in which the perpetrator resides. This exact transnational nature of cybercrime challenges traditional methods of investigating criminal activity, tracking, trying and rehabilitating offenders[49]. Most importantly, transnational cybercrime puts into question traditional notions of jurisdiction and requires cooperation of criminal justice systems, instruments, organs and agents across the globe.

States' jurisdiction

The most important thing that must be secured before a cyberattack-offender is brought before a state's legal system is jurisdiction. Jurisdiction refers to the power governments have to properly exercise authority (make laws and enforce them) within their territory50. In other words, jurisdiction is strongly linked to sovereignty and provides states with the power and authority to define and preserve the duties and rights of people within its territory, enforce laws, and punish violations of laws51.

Sovereignty is the starting point for state jurisdiction and international collaboration. Rules of customary public international law (meaning unwritten rules, customs respected by all states) safeguard nations' sovereign equality. These include the prohibition on states interfering in the internal and external affairs of other countries in any form or for any cause.52

Because law enforcement and criminal justice concerns come under the exclusive authority of the sovereign state, criminal jurisdiction has historically been connected to geographic territory. As a result, nations must avoid exerting pressure on other states over the behavior of specific national entities, such as law enforcement or the judiciary. It is possible that no

[49] Abid A. Adonis, *International Law on Cyber Security in the Age of Digital Sovereignty,* November 2019 Sciences Po, France https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/

[50] Legal Information Institute, Cornell Law School https://www.law.cornell.edu/wex/jurisdiction

[51] https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html

[52] States have sovereignty and territorial integrity and can freely determine their own political, economic, cultural and social system. See *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States*, annex to GA resolution A/RES/20/2131 (XX), 21 December 1965, *the Corfu Channel case*, the Military and Paramilitary Activities case, International Court of Justice.

one will be detained, neither any summons will be issued, and no police or tax investigations will be conducted, unless under the provisions of a treaty or other agreement, mounted on the territory of another state provided.53 Of course, not all crimes take place inside the boundaries of the territorial jurisdiction. When this occurs, international law has grown to recognize a number of bases for extraterritorial criminal jurisdiction.

As stated before, states primarily claim jurisdiction over crimes committed within their territory (principle of territoriality). Territorial sovereignty can be obviously applied to cyberspace, particularly to states' information and communications technology (ICT) infrastructure54; state sovereignty may be violated when third parties gain unauthorized access to ICT in foreign countries without the knowledge and permission of the host country and/or its law enforcement agents.

Cybercrime jurisdiction is established by other factors as well, such as the nationality of the offender and/or the victim (principle of nationality; active and passive personality principles respectively), and the impacts of the cybercrime on the interests and security of the state (protective principle)55. Cybercrime jurisdiction is established by national cybercrime laws.

The table below summarizes the most common legal basis found in national legislation and international agreements. A wide notion of necessity that the offence and the state exercising jurisdiction have a "sufficient relationship" or "real link" is common to all of these criteria.

[53] Brownlie, I., 2003. Principles of Public International Law. 6th ed. Oxford: Oxford University Press. p.306.

[54] Article 22(1) of the Council of Europe's Convention on Cybercrime of 2001, states that "[e]ach Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence … [included in] this Convention, when the offence is committed … in its territory."

[55] https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html

Principles of Criminal jurisdiction

Principle of territoriality (Objective territorial principle)	Even if the perpetrator is a foreign citizen, a state can punish acts that occur on its territory. Even though the perpetrator is located outside of the territory, territorial jurisdiction applies if one of the offence's basic parts, and notably its effects, occur within the territory. The objective territoriality concept ensures that the accused offender can be tried in both the state where the behavior commenced and the state where the offence was concluded.[56]
Effects Doctrine	Foreign behavior that has a significant impact on the territory is susceptible to jurisdiction.
Principle of Nationality	Jurisdiction is established depending upon the nationality of the individual concerned16
(Active)	Jurisdiction is established based on the nationality of the offender, wherever the crime is committed
(Passive)	Jurisdiction is established based on the nationality of the victim, wherever the crime is committed
Habitual residence	Jurisdiction is established based on the place of habitual residence of the offender
Protective principle	When a criminal conduct committed outside of the country jeopardizes the state's security and/or threatens its vital interests, jurisdiction is established.

[56] Lotus case, PCIJ, Series A, No. 10, 1927, 23, 30.

Principle of universality	Regardless of the region or nationality of the persons involved, jurisdiction is created over anybody suspected of committing a small number of "international crimes," such as piracy, war crimes, or severe violations of the Geneva Conventions. When a state with territorial jurisdiction is unable or unwilling to prosecute, the concept is typically used.

Countries & Organizations Involved

Examples of national mechanisms against cybercrime

Organizations in a variety of industries are becoming increasingly vulnerable to cyberattacks, putting the private information of millions of individuals at stake. Hackers, criminals, and hostile foreign groups aim to disrupt government agencies, spread distrust, and gain classified or sensitive information.

United States of America[57]

When cyberwarfare is on everyone's mind in the West, the United States uses a distinct "tone of voice." The US offers security strategies solely in response to cyberwarfare, essentially going on the defensive when sophisticated cyber techniques are used against them. The Department of Homeland Security, the Federal Bureau of Investigation and the Department of Defence are all responsible for cybersecurity in the United States. In recent years, a new department called Cyber Command was established to deal exclusively with cyber threats.

Cyber Command is a US Strategic Command military subcommand in charge of dealing with threats to the military's cyber infrastructure. Army Forces Cyber Command, the Twenty-fourth Air Force, Fleet Cyber Command, and Marine Forces Cyber Command are among the military parts of Cyber Command. It guarantees that the President can traverse and manage information networks, as well as having military alternatives accessible if the nation's defense has to be carried out in cyberspace. State and non-state actors who are developing cyberwarfare capabilities in order to undertake cyber espionage and other assaults against the United States and its allies must be monitored by Cyber Command personnel. Cyber Command aims to provide a deterrent to prospective enemies targeting the United States, as well as a multi-faceted agency capable of conducting its own cyber operations.

All in all, by investigating a wide range of cybercrimes, from theft and fraud to child exploitation, and apprehending and prosecuting those guilty, law enforcement plays a critical role in accomplishing USA's cybersecurity goals. The Department of Homeland Security (DHS) collaborates with other federal agencies to conduct high-impact criminal investigations in

[57] https://obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime/threat

order to disrupt and defeat cyber criminals, prioritize technical expert recruitment and training, develop standardized methods, and widely share cyber response best practices and tools.

Finland

The Government of Finland represents the highest level of cyber security management. The Government is responsible for providing political guidance and strategic guidelines for cyber security as well as for taking the required decisions regarding the resources and prerequisites to be allocated to it.

China

Though no universal definition of cyber warfare exists, a study conducted by the RAND Corporation is widely cited by Chinese military analysts: cyber warfare is strategic warfare in the information age, much as nuclear warfare was in the twentieth century. This concept is used to suggest that cyber warfare is far more important to national security than previously thought, and that it entails rivalry in areas other than the military, such as economics, diplomacy, and social development.

The major objectives of cyber capabilities, according to China's Military Strategy, are "cyberspace situation awareness, cyber defense, support for the country's cyberspace efforts, and involvement in international cyber cooperation."[58] These goals are framed in the policy as “preventing catastrophic cyber disasters, guaranteeing national network and information security, and preserving national security and social stability.”

South Africa

South Africa now meets international cybercrime standards thanks to a new law. It couldn't come soon enough, given the global rise in internet-based crimes, which is partially attributable to more individuals working from home owing to the COVID-19 epidemic. The country's well-developed financial infrastructure makes it a desirable target for cyber criminals who use the internet to commit extortion, fraud, child pornography, human trafficking, and the sale of illegal products.

South Africa's Cybercrimes Act, according to Advocate Doctor Mashabane, is a "groundbreaking and decisive move in the country's cyber governance and policy arena." Mashabane is the former South African Cyber Envoy to the United Nations and the Director-General of the Department of Justice and Constitutional Development. The new cyber legislation, together with the Protection of Personal Information (POPI) Act 2020, which will take effect on 30 June 2021, is an important element of South Africa's arsenal in the battle against cybercrime.

[58] https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734

Examples of states that face serious threats due to cybercrime

Russian Federation

Approximately 25 million cyber assaults on IT infrastructure were fought and halted by Russia during the 2018 FIFA World Cup. In June 2019, Russia said that it is "probable" that the US is hacking into its electrical system. According to the New York Times, American hackers from the US Cyber Command placed malware capable of damaging the Russian electrical system. The US Justice Department accused six Russian military officials on October 19, 2020, with participating in a global cyber effort that targeted the French election, the 2018 Winter Olympic Games opening ceremony, US corporations, and Ukraine's electricity grid. For the massive disruption it created, the campaign was estimated to have cost billions of dollars.

Albania

Albania's Minister of Defense, Niko Peleshi, has announced the establishment of a Cyber Defense Unit in response to the country's increasing number of cyberattacks.

“We are a NATO country in the region; we have rivals and competitors. Certain interests meet and want to destabilize our constitutional order and our defense system, or even test our reaction against these attacks,” said Peleshi.59

It isn't just the government, he claims, that is under attack. Hackers and ransomware are also a problem for private businesses. When hackers obtain access to a company's computer system, they demand a huge quantity of money to restore it to its previous state. He stated that the country's defensive capabilities were "limited," but that the Ministry of Defense planned to build up a Cyber Defense Unit with US assistance.

Peleshi did not provide any further information on the unit or when it will be operating. It's also uncertain whether this unit will do anything to stop Albania's massive number of assaults. The country is now Europe's fifth-largest source of cybercrime, accounting for 11.79 percent of all cyberattacks throughout the continent.

India VS. Pakistan

Two such incidents involving cyberspace conflicts between India and Pakistan occurred in the 1990s. Previous cyber-attacks were first reported in 1999. Since then, India and Pakistan have been embroiled in a lengthy conflict over Kashmir that has spilled over into cyberspace. According to historical sources, each country's hackers have frequently attacked the other's computing database system. The number of assaults has increased year after year: 45 in 1999, 133 in 2000, and 275 as of August 31, 2001. In 2010, Indian hackers known as the "Indian Cyber Army" launched a cyber-attack against at least 36 government database websites. In an attempt to extract critical database information, Indian hackers attacked the official

[59] https://exit.al/en/2021/07/13/albania-to-launch-cyber-defense-unit-to-tackle-growing-online-threats/ Albania to Launch Cyber Defense Unit to Tackle Growing Online Threats

website of Pakistan's Election Commission in 2013. In response, Pakistani hackers dubbed "True Cyber Army" attacked and vandalized 1,059 websites related to Local elections.

For a more realistic approach to the issue you can click here to view a live Cyber Threat Attack Map60.

UN Involvement

United Nations Convention against Transnational Organized Crime

The United Nations Convention Against Transnational Organized Crime (UNTOC)[61] was established in 2000. It began as a treaty between Member States before being adopted by the General Assembly later that year, transforming it into a complete UN convention. Within the topic of transnational organized crime, this historical development highlighted three primary areas of significance: human trafficking, migrant smuggling, and illegal weapon trafficking. The success of achieving the Millennium Development Goals, and later the Sustainable Development Goals has been influenced by each problem listed in the UNTOC.

This is due to organized crime's persistent socioeconomic destabilizing consequences. Drug networks, human trafficking, and arms trafficking, for example, can have an influence on a region's peace and security, human rights abuses, and social and economic development chances. Women are disproportionately affected by this crime since they are the principal victims of the worldwide sex slave trade.

Undoubtedly cybercrimes are regarded as modern types of transnational organised criminal offences[62]. Despite that, the UNTOC does not exclusively cover cyber-related issues. ALthough important guidelines are given through the UNTOC, cybercrimes cannot be effectively tackled without a convention solemnly dedicated to cybersecurity measures.

While a number of countries have been pushing for a global convention under the auspices of the United Nations, and the Russian Federation has in particular proposed a "Draft United Nations Convention on Cooperation in Combating Cybercrime" in 2017 (A/C.3/72/12), to date international consensus on such a global convention within the framework of the United Nations is still insufficient.

United Nations Office on Drugs and Crime

The United Nations Office on Drugs and Crime (UNODC) is a global leader in the battle against illegal drugs and international crime. UNODC was founded in 1997 as a result of a merger between the United Nations Drug Control Programme and the Centre for International Crime Prevention. It operates through a global network of field offices in all areas of the globe. For 90% of its funding, the UNODC relies on voluntary contributions, primarily from governments.

[60] https://www.imperva.com/cyber-threat-attack-map/
[61] https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html
[62] https://www.unodc.org/unodc/en/cybercrime/index.html

UNODC is tasked to support Member States in their fight against illegal drugs, crime, and terrorism. Member States also decided in the Millennium Declaration, and later on in the SDG's 2030 Agenda, to step up efforts to combat transnational crime in all of its forms, to redouble efforts to carry out the commitment to combat the global drug issue, and to take coordinated action against international terrorism.

To assist countries in drafting requests for mutual assistance, the United Nations Office on Drugs and Crime (UNODC) created a *Mutual Legal Assistance Request Writer Tool.* Additionally, in accordance with the General Assembly resolution 65/230 and the UNODC's Commission on Crime Prevention and Criminal Justice resolutions 22/7 and 22/8, the *Global Programme on Cybercrime* is mandated to assist Member States in their struggle against cyber-related crimes through capacity building and technical assistance.

Other relevant Intergovernmental Organizations (IGOs)

INTERPOL

Apart from the UN, INTERPOL is another intergovernmental organization whose function has been proven valuable in combating cyberattacks on an international level. INTERPOL acts as a communication hub between countries, helping to disseminate information, such as *notices*, and even assisting in coordinated operations between countries. INTERPOL does not have the authority to arrest criminals; it can rather help with the creation of a *Joint Investigation Team* (just like Europol does.) that can assist in criminal investigations, but only local investigators have the authority to make arrests locally[63]. More specifically, INTERPOL has created two secure and flexible communication platforms for police and other stakeholders:

- **Cybercrime Knowledge Exchange workspace**[64], which handles general, non-police information and is open to all relevant users;
- **Cybercrime Collaborative Platform – Operation**[65], to support law enforcement operations, with access restricted to operational stakeholders only.

[63] https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/informal-international-cooperation-mechanisms.html
[64] https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-Collaboration-Services
[65] https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-Collaboration-Services

International Cooperation

Exactly because cybercrime has an undeniable transnational nature, sometimes international cooperation may be the only way to serve justice. International cooperation depends on harmonized national substantive cybercrime laws, which criminalize cybercrime, and national procedural cybercrime laws that set the rules of evidence and criminal procedure. International cooperation can also be facilitated by harmonizing, wherever needed, bilateral, regional, and multilateral instruments on cybercrime. International cooperation is further facilitated by bilateral, regional, and multilateral cybercrime as long as a clause requiring the alleged conduct to be considered illegal in cooperating countries exists (*dual criminality*)[66].

There are several cybercrime and cybercrime-related treaties, laws and directives[67]:

- A case in point is the **Council of Europe's Convention on Cybercrime** of 2001. This Convention seeks to harmonize the national laws of signatory-states, improve cybercrime investigation techniques, and promote international cooperation on the field of cybersecurity.
- The **Commonwealth of Independent States' Agreement on Cooperation in Combating Offences related to Computer Information** of 2001.
- The **Arab Convention on Combating Information Technology Offences of 2010**, signed by Arab League's Member states..
- **The Shanghai Cooperation Organization's Agreement on Cooperation in the Field of International Information Security** of 2010.
- **The African Union Draft Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa (Draft African Union Convention)** of 2012.
- **The African Union Convention on Cyber Security and Personal Data Protection** of 2014.

Possible Solutions

The measures implemented to counter organized cyber-crime have focused on law enforcement and prosecution efforts, technical solutions, and education campaigns[68].

1. Law enforcement

a. General cybersecurity regulations

i. Micro level

Cyberattacks should firstly be directed on a micro level, meaning by each government. We should not forget that cybercrime can be not only transnational but a simple criminal offence that can be dealt with by domestic organs and instruments. Later on, further analysis is provided on measures such as public education regarding the safe

[66] https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html
[67] https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-and-regional-instruments.html
[68] https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/preventing-and-countering-cyber-organized-crime.html

usage of the internet, police's training on detecting cyberattacks. Apart from those, each government should secure transparency in its systems. Lastly, nations need to find ways of implementing security methods without breaching the users' privacy, an idea that is also later discussed.

ii. Macro level

The international community must strongly and officially re-define its policy against cyberwarfare via an international agreement negotiated and voted upon by all nations. Cyber Warfare and transnational cyber organised offences against any government's national security and sovereignty need serious attention and their confrontation should be regarded as part of internationally agreed protocol. Cybersecurity should be further addressed in international fora like the Security Council, the UNODC, the GA1 Committee.

b. Data related issues

The international community shall ensure that during the efforts to combat cyberattacks, freedoms and privacy should be equally protected as freedom and privacy. Member nations, however, have different views on the issue. It is, thus, necessary for international organizations such as the UN to provide intervention, guidance and suggest a common strategy to be adopted by all nations, so as to safeguard human rights. For instance, the EU's initiative to form the GDPR protocol is a notable example of a balancing policy.

2. Prosecution

Prosecutions of cyber organized criminals are aimed at holding perpetrators of illegal activities responsible for their crimes. The transnational nature of cybercrimes puts into question traditional prosecution methods; cooperation between states is therefore deemed necessary. As stated before, INTERPOL has been acting as a "mediator" that creates a communication platform for states to share information and practices. Such efforts need to be further promoted and enhanced so as to reduce bureaucratic obstacles. It would be also helpful if an international framework - ideally in the form of a treaty- for the collaboration of governments in prosecution projects was established.

3. Technical Methods

Ethical hacking, often known as "white hat hacking," composed by a security specialist group that makes a legitimate attempt to obtain illegal access to a computer system, application, or data. They contribute to an organization's security posture by being proactive. The objective of ethical hacking differs from harmful hacking in that it requires prior consent from the company or owner of the IT asset. Governments as well as private companies shall invest in ethical hacking as it has proven to be a very successful method.

Additionally, training the police on cybersecurity should be a priority as well. Governments in cooperation with INTERPOL could organise workshops, seminars (regarding the basic structure of an organized crime, basics of ethical hacking, programming languages,

cyberwarfare both on each country and transnationally, how to secure important government documents) and training programmes for police officers and computer experts would be a vital step in combating cybercrime.

The development of sophisticated software and hardware solutions should be a priority for governments and private companies. Such measures should be taken as well by companies that produce everyday technological devices and systems. For instance, it should be mandatory for all personal computers, phones and other technological devices to have malware prevention systems installed as standard means to prevent viruses and hackers. Public and private networks could, similarly, have standard protection against malware and hackers. Such software should be updated regularly without any cost, so as to adapt to new circumstances.

Facial recognition technology has been particularly used to identify trafficked persons, sexually exploited children and sexual abuse material in general. Image recognition software can be further used to identify in images illicit goods that have been illegally traded, such as drugs or firearms.

4. Raising Awareness

Education campaigns have been severally used as a tool of (cyber) crime prevention and have focused on raising awareness on cyber organized crime. Informing the public about the ways in which individuals can protect themselves from cybercrime, such as fraud, malware, sexual exploitation etc. is a key measure to combat and prevent cybercrime from an early stage.

Bibliography

Note: *Chicago-style citation was not possible for certain sources. Please make sure to also check the footnotes within the Study Guide.*

(www.dw.com), Deutsche Welle. "'Largest Illegal DARKNET Marketplace' DarkMarket Taken Offline: Dw: 12.01.2021." DW.COM. Accessed September 9, 2021. https://www.dw.com/en/largest-illegal-darknet-marketplace-darkmarket-taken-offline/a-56200737

"4 Arrested in Takedown of Dark Web Child Abuse Platform with Some Half a Million Users." Europol, June 1, 2021. https://www.europol.europa.eu/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-million-users

"After the Retrospective: Dyn DDoS." Gremlin, October 28, 2019. https://www.gremlin.com/blog/after-the-retrospective-dyn-ddos/

"Automating Cyber Attacks." Center for Security and Emerging Technology, June 22, 2021. https://cset.georgetown.edu/publication/automating-cyber-attacks/

"Business Home." McAfee. Accessed September 9, 2021. https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html

"Caesar Cipher." Wikipedia. Wikimedia Foundation, May 20, 2021. https://en.wikipedia.org/wiki/Caesar_cipher

"Combating Foreign Influence." FBI. FBI, August 30, 2018. https://www.fbi.gov/investigate/counterintelligence/foreign-influence

"Core War: Creeper and Reaper." Creeper & Reaper. Accessed September 7, 2021. https://corewar.co.uk/creeper.htm.

"Dark Web Hitman Identified through Crypto-Analysis." Europol, May 1, 2021. https://www.europol.europa.eu/newsroom/news/dark-web-hitman-identified-through-crypto-analysis

"DarkMarket: World's Largest Illegal Dark Web MARKETPLACE Taken Down." Europol, February 1, 2021. https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down

"Double Blow to Dark Web Marketplaces." Europol, June 1, 2019. https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces

"Head of Iran's Atomic Energy Body Resigns." Reuters. Thomson Reuters, July 16, 2009. https://www.reuters.com/article/uk-iran-nuclear-resignation-sb/head-of-irans-atomic-energy-body-resigns-idUKTRE56F2CM20090716?edition-redirect=uk

"ICS Joint Security Awareness Report (JSAR-12-241-01B)." Cybersecurity and Infrastructure Security Agency CISA. Accessed September 7, 2021. https://us-cert.cisa.gov/ics/jsar/JSAR-12-241-01B.

"Interpol/Crimes/Cybercrimes". Accessed September 1, 2021 https://www.interpol.int/en/Crimes/Cybercrime

"Mastermind behind EUR 1 BILLION CYBER Bank Robbery Arrested in Spain." Europol, April 1, 2018. https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain

"Moonlight Maze - An Overview." Moonlight Maze - an overview | ScienceDirect Topics. Accessed September 9, 2021. https://www.sciencedirect.com/topics/computer-science/moonlight-maze

"Most Popular Types of Cryptocurrency | Nextadvisor with Time." Time. Time, July 15, 2021. https://time.com/nextadvisor/investing/cryptocurrency/types-of-cryptocurrency/#cryptocurrencies

"Significant Cyber Incidents." Significant Cyber Incidents | Center for Strategic and International Studies. Accessed September 6, 2021. http://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

"Silk Road." Encyclopædia Britannica. Encyclopædia Britannica, inc. Accessed September 9, 2021. https://www.britannica.com/topic/Silk-Road-trade-route

"Solar Sunrise." The IT Law Wiki. Accessed September 7, 2021. https://itlaw.wikia.org/wiki/Solar_Sunrise.

"Spyware - What Is It & How to Remove It?" Malwarebytes. Accessed September 9, 2021. https://www.malwarebytes.com/spyware

"Stuxnet Analysis BY Langner, Based on Reverse Engineering of the Payload." Langner. Ralph Langner, July 23, 2020. https://www.langner.com/stuxnet/

"The Melissa Virus." FBI. FBI, March 25, 2019. https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519

"The Tor Project: Privacy & Freedom Online." Tor Project | Anonymity Online. Accessed September 9, 2021. https://www.torproject.org/

"The Tor Project: Privacy & Freedom Online." Tor Project. Accessed September 9, 2021. https://www.torproject.org/about/history/

"Understanding the Dyn Ddos Attack." NCTA. Accessed September 9, 2021. https://www.ncta.com/chart/understanding-the-dyn-ddos-attack?share_redirect=%2Ftopics#colorbox=node-2825

"United Cyber Caliphate (Ucc / Islamic State - Isis)." TRAC. Accessed September 9, 2021. https://www.trackingterrorism.org/group/united-cyber-caliphate-ucc-islamic-state-isis

"University Module Series Cybercrime" Education for Justice (E4J) in collaboration with the United Nations Office on Drugs and Crime (UNODC). Accessed September 1. 2021 https://www.unodc.org/e4j/en/tertiary/cybercrime.html

"UPDATE 2-Iran Says Cyber Foes CAUSED Centrifuge Problems." Reuters. Thomson Reuters, November 29, 2010. https://www.reuters.com/article/iran-ahmadinejad-computers-idAFLDE6AS1L120101129.

"What Is A Keylogger?: How to Detect Keystroke Loggers." Malwarebytes. Accessed September 9, 2021. https://www.malwarebytes.com/keylogger

"What Is Social Media Warfare?" PREVENCY®, June 15, 2020. https://prevency.com/en/what-is-social-media-warfare/

Abid A. Adonis. "International Law on Cyber Security in the Age of Digital Sovereignty" November 2019, Sciences Po, France. Accessed September 2, 2021 https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/

Allen Karen "South Africa lays down the law on cybercrime" Institute for Security Studies, June 9, 2021, Accessed September 1, 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime

Bloomenthal, Andrew. "Inside the Dark Web." Investopedia. Investopedia, September 4, 2021. https://www.investopedia.com/terms/d/dark-web.asp

Buchanan, Ben, John Bansemer, Dakota Cary, Jack Lucas, and Micah Musser. "Automating Cyber Attacks," 2020. https://doi.org/10.51593/2020ca002

Burdova, Carly. What is a rootkit and how to remove it? Avast, August 11, 2021. https://www.avast.com/c-rootkit

Burnham, Kristin. "Artificial Intelligence vs. Machine Learning: What's the Difference?" Northeastern University Graduate Programs, November 10, 2020.

https://www.northeastern.edu/graduate/blog/artificial-intelligence-vs-machine-learning-whats-the-difference/

European Treaty Series – No. 185 "Convention on cybercrime" Council of Europe November 23, 2001. Accessed September 2, 2021 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561

Frankenfield, Jake. "Cryptocurrency." Investopedia. Investopedia, August 23, 2021. https://www.investopedia.com/terms/c/cryptocurrency.asp

Frankenfield, Jake. "Silk Road Definition." Investopedia. Investopedia, September 8, 2021. https://www.investopedia.com/terms/s/silk-road.asp

Johansen, Alison Grace (for NortonLifeLock). "What Is a Trojan? Is It a Virus or Is It Malware?" Norton. Accessed September 9, 2021. https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html

Kaspersky. "Tips on How to Protect Yourself against Cybercrime." www.kaspersky.com, July 5, 2021. https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

Kaspersky. "What Is the Deep and Dark Web?" www.kaspersky.com, August 23, 2021. https://www.kaspersky.com/resource-center/threats/deep-web

Kushner, David. "The Real Story of Stuxnet." IEEE Spectrum. IEEE Spectrum, July 29, 2021. https://spectrum.ieee.org/the-real-story-of-stuxnet#toggle-gdpr.

Kushner, David. "The Real Story of Stuxnet." IEEE Spectrum. IEEE Spectrum, July 29, 2021. https://spectrum.ieee.org/the-real-story-of-stuxnet

Langner, Ralph. "Cracking Stuxnet, a 21ST-CENTURY Cyber Weapon." TED. Accessed September 9, 2021. https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyber_weapon

Newman, Lily Hay. "A 1.3-Tbs Ddos Hit Github, the Largest Yet Recorded." Wired. Conde Nast, March 1, 2018. https://www.wired.com/story/github-ddos-memcached

Seals, Author: Tara, and Tara Seals. "2.28M MeetMindful Daters Compromised in Data Breach." Threatpost English Global threatpostcom. Accessed September 9, 2021. https://threatpost.com/meetmindful-daters-compromised-data-breach/163313/

Sean Gallagher - Oct 23, 2011 11:00 pm UTC. "Anonymous Takes down Darknet Child Porn Site on Tor Network." Ars Technica, October 23, 2011. https://arstechnica.com/information-technology/2011/10/anonymous-takes-down-darknet-child-porn-site-on-tor-network/

Taylor Alice, Albania to Launch Cyber Defense Unit to Tackle Growing Online Threats" Exit news, July 7, 2021, Accessed September 1, 2021. https://exit.al/en/2021/07/13/albania-to-launch-cyber-defense-unit-to-tackle-growing-online-threats/

Team, SecureWorld News. "Moonlight Maze Lives On? Researchers FIND 20-Year-Old Link to Current Apt." Cybersecurity Conferences & News. Accessed September 9, 2021. https://www.secureworld.io/industry-news/moonlight-maze-lives-on-researchers-find-link-to-current-apt

The White House,"Strategy to combat Transnational Organised Crime". National Security Council. 25 July 2011. Accessed September 1, 2021. https://obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime

Turton, William, and Kartikay Mehrotra. "Hackers Breached Colonial Pipeline Using Compromised Password." Bloomberg.com. Bloomberg, June 4, 2021. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

UN "United Nations Convention on Transnational Organized Crime". Entry into force: 29 September 2003. Accessed September 1 2021 https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

UNODC "Comprehensive Study on Cybercrime" Draft February 2013. Accessed September 1 2021 https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

UNODC "United Nations Office on Drugs and Crime / Cybercrime". Accessed 1 September 2021 https://www.unodc.org/unodc/en/cybercrime/index.html

Vick, VIPRE. "What Is a Worm Virus?" VIPRE, April 21, 2017. https://www.vipre.com/resource/what-is-a-worm-virus/

Volz, Dustin. "Cyber Attack Eases, Hacking Group Threatens to Sell Code." Reuters. Thomson Reuters, May 15, 2017. https://www.reuters.com/article/us-cyber-attack-idUSKCN18B0AC

Westby, Jody. "Russia Has Carried Out 20-Years of Cyber Attacks That Call for International Response." Forbes. Forbes Magazine, December 20, 2020. https://www.forbes.com/sites/jodywestby/2020/12/20/russia-has-carried-out-20-years-of-cyber-attacks-that-call-for-international-response/