Cyber Conflict and Cyber Strategy

This learning unit introduces the hierarchy of cyber threats, describes the aggressive and defensive capabilities of various actors, and examines the international legal framework and options available to improve cyber security in military and civilian contexts.

Niklas Schoernig
Peace Research Institute Frankfurt (PRIF)

Tommaso de Zan
University of Oxford

Cite as: Niklas Schoernig and Tommaso de Zan, "Cyber Conflict and Cyber Strategy" in EUNPDC eLearning, ed. Niklas Schoernig, Peace Research Institute Frankfurt. Available at https://eunpdc-elearning.netlify.app/lu-19/, last modified 4 December 2025

The EU Non-Proliferation and Disarmament eLearning Course aims to cover all aspects of the EU non-proliferation and disarmament agenda. It's produced by PRIF with financial assistance of the European Union. The contents of individual learning units are the sole responsibility of the respective authors and don't necessariy reflect the position of the European Union.

Funded by
the European Union

1. A Message from the Authors

Hello there, my name is Niklas Schörnig and I am head of the Peace Research Institute Frankfurt Research Group on Emerging Technologies, Order and Stability.

Hi, my name is Tommaso De Zan and I am a PhD candidate in Cyber Security at the University of Oxford. I also regularly collaborate with **ENISA**, the EU Cyber Security Agency, on topics related to the cyber security skills shortage and skills development.

In this learning unit, we will guide you through the confusing fields of security-related cyber incidents. The first chapter, where I will be your host, focuses on **conceptual work** and **definitions**, as well as legal aspects of cyber incidents. The second chapter gets more technical and looks at the **differences between classical weapons and cyber weapons** and why these differences have a severe impact on the implementation of classical arms control concepts.

I will then take the lead in chapters 3, 4 and 5. In chapter 3, I will analyse the **cyber defence strategies** of major international players, including China, Russia, the UK and the US. In addition, I will explain how **cyber operations** are often part of wider information warfare strategies. In chapter 4, I will discuss the threat of cyber terrorism and threats to critical national infrastructure. I will talk extensively about the operations of two designated terrorist organisations such as **ISIL/Daesh** and **al-Qaeda** and how they have been thwarted by the US cyber command. Finally, in chapter 5, I will talk about **EU cyber security policies**, with a particular focus on measures in the foreign, security and defence realms.

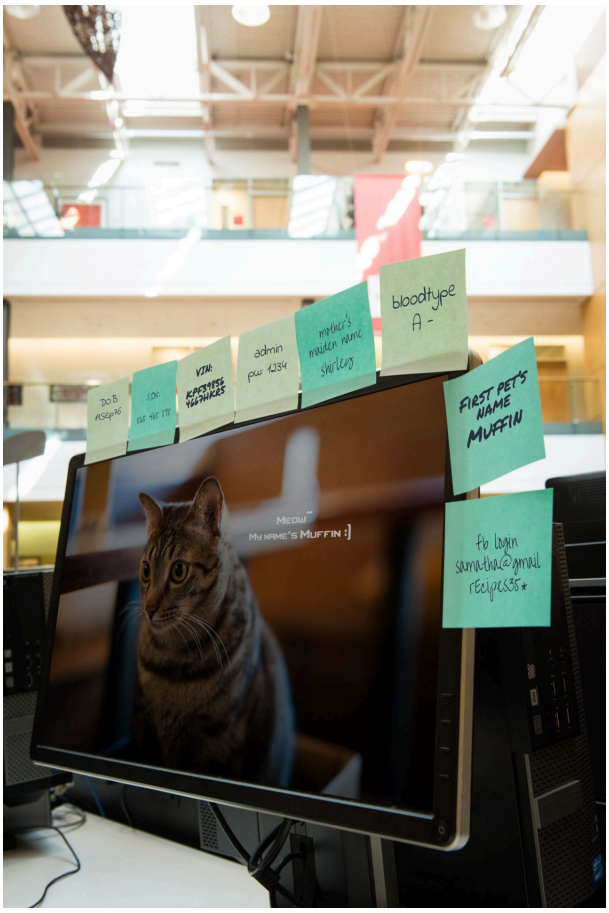
We hope that you will enjoy our learning unit.

2. What is Cyber Warfare?

Cybersecurity

Cybersecurity has become one of the buzzwords of our time. On a very general level, it describes **all measures and practices protecting and defending computer networks, servers, computers** – basically all computerized items, e.g. modern cars, planes, smart homes – from infiltration to hostile takeover.

Cybersecurity also includes setting up **processes** and making **decisions**, e.g. about access rights, or planning for the – hopefully unlikely – case of a disaster, that is a severe security breach with or without the loss of data. The basic aim would be to continue work with as few restrictions as possible and be "resilient".



The Era of Oversharing (pt.1), https://cltc.berkeley.edu/cybervisuals/. Most cyber incidents happen due to untrained users.
Bronney Hui (CC BY 4.0)

Finally, cybersecurity also includes the **training of users** in such things, for example, as preventing posting passwords on the screen for everyone to see.

Depending on the source, roughly 50 to 90 percent of all cyber incidents can be attributed to uninformed or untrained staff.

In some cases, cybersecurity means **monitoring networks** in real time, in other cases it focuses on **checking applications** for glitches in the design phase before release or patching them afterwards. It can mean the protection of data from manipulation or deletion.

From Cybersecurity to "Cyberwar"

Malware attacks, or intrusions, in civilian as well as military networks often share the same tools. Overall cybersecurity is relevant for **private users, businesses** and **scientific institutions**, and **government agencies** such as ministries, executive bodies and the military.

Cybersecurity is thus essential to guarantee that normal civilian life and business continue, it is the defensive side of cyberoperations.

While we will cover some aspects of civilian cybersecurity in this learning unit, the focus is on the **military use of cybertools** as a means to influence a conflict in one's direction – or the offensive side, if you will.

We will look at different forms of malicious cyberoperations, with a clear focus on the military use of cybertools. While many would use the word cyberwarfare in that context, using the term "cyberwar" is not without problems.

Malicious Cyberoperations – a Taxonomy

This video …

- **explains** why it is hard to find a definition for cyberattacks and cyberwar
- **discusses** why the word "war" might be misplaced in relation to the cyber-realm most of the time
- **introduces** different forms of cyber incidents
- **distinguishes** between cyber operations and information operations in the cyber space

In 1993, John Arquilla and David Ronfeldt published a seminal article titled "Cyberwar is coming!" – and they put an exclamation mark at the end. Many observers were sceptical at that time and thought this to be an exaggeration – a science-fiction fantasy.

18 years later, in 2011, the US Department of Defense upgraded **cyberspace** to the status of a so called "operational domain", placing cyber on the same level as land, sea, air and space. Concurrently, in 2012 Thomas Rid declared "Cyber War Will Not Take Place", a perspective he has reiterated in several texts until today.

Unfortunately, internationally agreed **definitions** for what actually constitutes a cyberwar are still lacking. When political scientists talk about war, they usually are guided by definitions like the one by the Uppsala Conflict Data Program, which defines war as "a state-

based conflict or dyad which reaches at least 1000 battle-related deaths in a specific calendar year." As we will see later, there has not been any cyber-related incident matching this definition.

But there is a tendency to exaggerate cyberthreats by unknowingly or knowingly using imprecise vocabulary. Especially the media, but also some decision makers, routinely use the term cyberwar for any unfriendly act against one's state information technology infrastructure. It is therefore important to differentiate between **different forms of malicious cyber operations**.

The probably most harmless form is called **"hacktivism"**. Examples would be the defacement of government websites, changing text or visual elements, or so-called Distributed Denial of Service attacks, where a website is overwhelmed by a flood of simultaneous server requests, disrupting normal functionality.

Another widespread form of non-state cyber activity is **"cybercrime"**. Everything with a clear criminal intention, including ransomware, that is the encryption of a victim's hard drive to demand ransom or phishing for passwords to commit identity theft, falls into this category.

A third form of cyber operation is **"cyberespionage"**, the collection of security relevant data by state actors, including, for example, blue prints of new weapon systems or "kompromat", that is compromising information suited for blackmail.

A fourth form is **"cyberterrorism"**, for example an attack against critical infrastructure like a traffic-light system or a nuclear power plant with the aim of causing uncertainty, fear and havoc, usually inflicting physical destruction and human casualties.

Finally, I would reserve the term **"cyberwar"** for a large-scale attack against military targets with the aim of supporting classical military kinetic attacks. From this perspective, a cyberwar is always supporting a comprehensive conventional military operation or attack. We will debate this in more detail when we look at the legal side of cyber operations.

Cyber Incidents in the Physical World so far (Selection)

2007 · Estonia

In late April 2007, many Estonian websites, including those of banks and governmental institutions, were flooded with denial-of-service attacks from millions of computers captured in 75 countries for several days. Estonia suspected that Russia was behind the attack or had at least assisted Russian 'patriotic hackers' as retaliation for the relocation of a Soviet-era grave marker.

However, these allegations could never be proven. The new NATO member Estonia turned to its Alliance partners for help, citing Article 5 of the Washington Treaty. However, after some deliberation the other NATO members concluded that collective defense as stated by Article 5 was not applicable, based on the same arguments fleshed out in the Tallinn Manual a few years later.

2007 · Syria: Operation Orchard

Shortly after midnight of September 6, 2007, fighter jets believed to belong to the Israeli Air Force (IAF) attacked a suspected nuclear reactor facility in Syria, destroying the site completely. According to news sources, Israeli intelligence had learned about the complex from a spying software planted on the computer of a senior Syrian government official.

In addition, experts suggested that the Syrian air defence had been spoofed with the help of a US-developed software called 'Suter'. This software made the Syrian systems believe that there was nothing out there to defend against. However, neither the bombing nor the use of cyber means has been confirmed.

2010 · Iran: Stuxnet

In 2010 security experts discovered a very sophisticated piece of malware, utilizing four previously unknown vulnerabilities as well as stolen security certificates. Instead of causing indiscriminate harm, this software, 'Stuxnet', was after something very special: a specific program controlling Siemens industrial hardware.

Coincidently, it was the exact software used for the enrichment centrifuges in Iran's highly controversial nuclear enrichment plant in Natanz. When the software reached Natanz it subtly altered the rotation speed of the centrifuges, not enough to be noticed, but enough to damage and break them eventually. It is believed that 'Stuxnet' was jointly programmed by Israeli and American experts to delay the Iranian nuclear program.

2015 · Germany: Attack on the German Bundestag
In 2015 a group of hackers penetrated the internal net of the German Bundestag, the German parliament, potentially getting hold of emails and confidential documents. German newspapers described the hack as a "spectacular intelligence operation". Only discovered by sheer chance, the offices of at least 16 MPs were compromised, including the Chancellor's (excepting the office at the Chancellery) and an unknown amount of information was retrieved.

After a comprehensive analysis, the German government was convinced that a branch of Russia's military intelligence agency with the nickname "Fancy Bear" was behind the attack. The penetration had been initiated by an email allegedly sent by the UN, containing a manipulated link, thereby fooling the Bundestag's firewall, ultimately installing a trojan on the respective computers. In 2020 chancellor Merkel reiterated that "she had 'hard evidence'" for Russia's responsibility.

2017 · WannaCry, NotPetya
WannaCry is a malware which started spreading in May 2017 and infected more than 230.000 Windows-based PCs in 150 countries on one day. It is a ransomware which, once activated, encrypts the hard drive and offers the user decryption keys in exchange for money. Victims of WannaCry included many public services and hospitals.

Another malware, called NoPetya, also seemingly ransomware, started spreading a month later, again targeting Windows based systems. This virus also spread by its own. In contrast to classical ransomware, it destroyed infected hard drive contents without a chance of recovery.

As the attack first targeted Ukraine, before spreading worldwide, many experts, as well as the governments of Ukraine, the US and the UK, suspected the source of NoPetya to be Russia. Russia rejected these allegations, pointing towards its own high number of infections.

2019 · Iran
After the spectacular drone attack against a Saudi-Arabian refinery in September 2019, allegedly conducted by Houthi rebels with Iranian help, as well as Iranian attacks against oil tankers in the Strait of Hormuz, the US launched cyberattacks against Iranian intelligence groups believed to be involved in the original attacks.

In contrast to what the military calls "kinetic attacks" the US government believes that the online operations conducted stayed well below the threshold of war, but still sent a deterring signal. US officials were hinting that other systems had been penetrated as well – including Iranian missile launch systems - thereby sewing suspicion that the systems would actually work when needed.

Forms of Cyber Operations

Not every malicious activity in the cyberrealm is a cyberwar. Many cyber operations fall into different categories and are conducted by different actors:

- **Hacktivism**
  - usually non-state actors
  - defacement of (government) websites
  - Distributed Denial of Service (DDoS) attacks
  - does not legitimize military self defence
- **Criminal Cyber Activities**
  - usually non-state actors
  - installing ransomware
  - identity theft
  - so-called '419 frauds'
  - industrial espionage
  - does not legitimize military self defence
- **Cyber Espionage**
  - usually state actors
  - copying of classified material
  - stealing of blue prints for weapon systems
  - hoarding of 'kompromat'
  - does not legitimize military self defence
- **Cyber Terrorism**
  - state or non-state actors
  - aims similar to classical terrorism
  - attacks against critical infrastructure with potentially devastating consequences
  - might legitimize military self defence
- **Cyber War**
  - state actors
  - no common definition
  - support for large scale conventional military operation
  - not a legal concept
  - might legitimize military self defence

Does International Law apply in the Cyber Realm?

This video debates:

- whether **international law** applies to the cyber realm
- why the so-called **Tallinn Manuals** are the most important yet inofficial publications in the issue

In the last video, we debated different forms of malicious cyber operations against a state's IT infrastructure. This has been an interesting exercise in conceptualization. Yet what concerns states most in this context is whether a specific type of attack warrants military self-defence. This leads to an important question: Is international law applicable to cyber threats?

As early as **1998**, the issue of cybersecurity was addressed by the UN General Assembly, based on a draft resolution by the Russian Federation. In **2003**, the UN established a multinational Group of Governmental Experts (GGE) on the issue of "Developments in the Field of Information and Telecommunications in the Context of International

Security". The question of the applicability of international law and international humanitarian law (IHL) was debated but contested, preventing consensus within the GGE on the issue and preventing a subsequent report. **Until today**, there have been six GGEs on the issue but only three agreed on a consensual report.

In **2013**, the report by the third GGE was the first to confirm that international law, as well as the UN Charter, are applicable to the cyber realm. Interestingly enough, this was also the bottom line of another 2013 document, the so-called **Tallinn Manual**. The Estonia-based NATO Cooperative Cyber Defence Centre of Excellence had initiated this non-binding study on cyber-conflicts and international law by an international group of experts. While it is not an official NATO document, it is one of the most significant publications on cyber conflict and international law so far, also confirming that the classical rules of international law remain applicable to the cyber-realm.

Regarding self-defence, the group of experts concluded "that cyber operations alone might have the potential to cross the threshold of international armed conflict". Notice that it says "might". While states do not have to condone less severe cyber operations against themselves, in most cases their reactions have to be restricted, or proportionate to the attack. The Tallinn-Manual defines a cyberattack as a cyber operation, that "is reasonably expected to cause injury or death to persons or damage or destruction to objects".

Given this **definition**, most of the cyber activities presented in the last video do not qualify as an attack in a legal sense. Even some forms of cyber-terrorism might not justify military self-defence, if, for example, they only cause substantial financial loss but not physical damage.

From the perspective of the Tallinn-Manual, cyberattacks have to match the effects of kinetic attacks in order to legitimize military self-defence. This position was reiterated in 2017, when **Tallinn 2.0** was published, focusing not only on interstate war, but other forms of conflicts as well.

Today, however, the 2013 consensus seems to be under jeopardy again. While Western states stick to the Tallinn argument, other actors like China and Russia argue that only selected aspects of international law are applicable to the cyber realm. **The debate is ongoing**.

The UN GGE Process and the 2015 Report

On the UN level, the issue of 'developments in the field of information and telecommunications in the context of international security' has been on the agenda since at least **1998**, starting with a Russian initiative. Since then, **annual reports** have been sent by the Secretary-General to the General Assembly focusing on national views.

In addition, **Groups of Governmental Experts** (GGEs) met five times, starting in **2004**, publishing three GGE-reports with and two without consensus. Currently the sixth GGE is meeting, probably presenting a concluding report in 2021.

Despite some problems, the GGE process has been widely acclaimed as an important forum to push the agenda of global cybersecurity.

Years	Resolution	Report
2004-05	A/RES/58/32 [https://www.undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F58%2F32&Language=E&DeviceType=Desktop&LangRequested=False]	No agreement
2009-05	A/RES/60/32 [https://www.undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F60%2F45&Language=E&DeviceType=Desktop&LangRequested=False]	Yes
2012-13	A/RES/66/32 [https://www.undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F66%2F24&Language=E&DeviceType=Desktop&LangRequested=False]	Yes
2014-15	A/RES/68/32 [https://www.undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F68%2F243&Language=E&DeviceType=Desktop&LangRequested=False]	Yes
2016-17	A/RES/70/32 [https://www.undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F70%2F237&Language=E&DeviceType=Desktop&LangRequested=False]	No agreement
2019-21	A/RES/73/32 [https://www.undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F73%2F266&Language=E&DeviceType=Desktop&LangRequested=False]	n/a

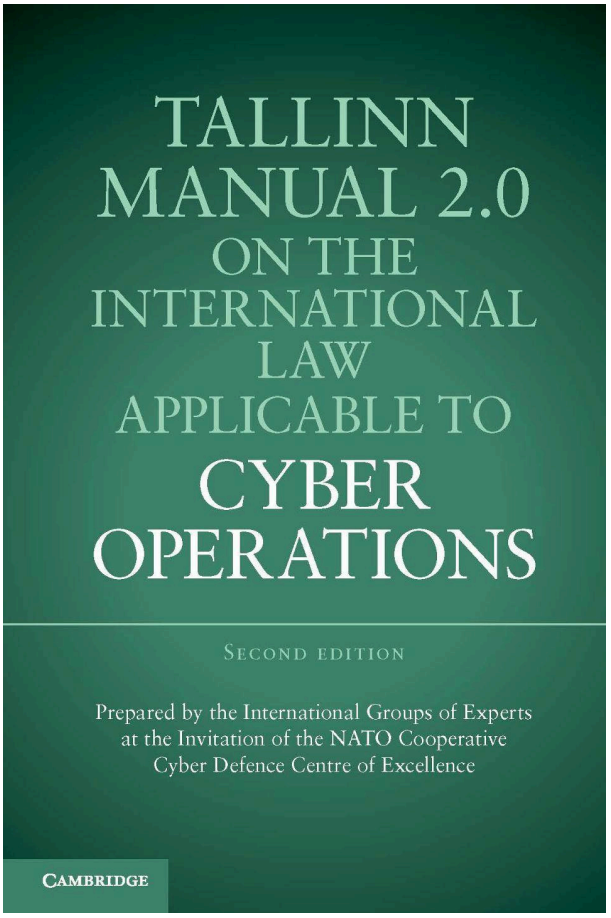
One problem, which has haunted the GGEs so far, has been the disagreement about the **scope of the issues to be debated**.

While China and Russia do not want the debates to be limited to cyber operations as debated in chapter one, but also to cover what they understand as foreign information operations, Western states have traditionally seen this as a threat to a free exchange of ideas and an uncensored internet.

Of the GGE reports, many experts find the report published in **2015** the most important as all 20 members of the GGE agreed on important principles, like the **protection of critical infrastructure**, the **exchange of information** in the case of an incident and the **refusal to let their territory be used for cyber attacks** by state or non-state actors – amongst others.

Currently, however, some observers at least feel that the GGE process is 'dead'. It will be important to see what the current GGE is able to achieve. Given the overall situation in arms control at the moment, it is doubtful whether a consensual report can be prepared.

The Tallinn Manual and Tallinn Manual 2.0



The Tallinn Manual 2.0, relased in 2017.

In addition to the UN GGEs, the **NATO Cooperative Cyber Defence Center of Excellence** (in Tallinn, Estonia) established another group of 19 law experts to debate the applicability of international law to cyber operations.

As a product of NATO countries, it is not endorsed by other states like Russia or China, which would prefer a more UN oriented action or other initiatives. However, NATO stresses that the manual is not an official document but the **opinion of independent experts**.

> A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.
>
> Tallinn Manual, Rule 30, p. 91-92

The first version of the manual was published in **2013**. Its focus was on interstate conflicts. A revised version (Tallinn 2.0) was released in **2017**, taking into account also other forms of cyberconflicts, for example between non-state actors and states.

However, the manual is very important as it was one of the first documents to conclude that **international law was applicable to the cyber realm**. In addition, it came up with a **legal definition** of **cyberattacks**.

Quiz

View quiz at `https://eunpdc-elearning.netlify.app/lu-19/`

3. Cyber arms control

New Problems Caused by the Cyber Realm

This video …

- gives a **basic idea** of how cyberattacks are conducted
- introduces the **"attribution problem"** in cyberspace
- shows why **deterrence** is problematic in the cyber realm
- explains the **difference between offensive and defensive cyber operations**
- introduces the concept of **"hackbacks"** and the problems they cause

What makes "cyber" special compared to the conventional realms of land, sea, air and space? One of the most important differences is how a **"cyber weapon"** actually works.

A conventional kinetic weapon causes damage by directing energy (such as heat, pressure or electromagnetic pulse), against a structure, a human body or electronic equipment. In contrast, a cyber tool has to work from the inside of its target – that is getting illegitimate software code to work on someone else's computer. **Access to the computer** is therefore key.

This can be done either by so-called "brute force" – trying endless name/password combinations to get access – or by using **knowledge about the relevant system**, its weaknesses and potential exploits. If, for example, a video player is used which is known to sometimes store data in dedicated areas of the computer's memory reserved for executable code, malformed inputs, that is specifically prepared – or weaponized – files, can force such a "buffer overflow" and execute malicious code. Usually this cannot be done "on the fly" – notwithstanding what Hollywood movies suggest – but requires a user to interact with the file: watch a prepared video, visit a specific website – etc. All necessary steps for a successful attack, from reconnaissance to achieving the objective, are described by the so-called **"kill chain"**, which will be presented later in the unit.

Another significant distinction between kinetic- and cyberattacks is that it is significantly harder to predict the **damage caused by the weapon**. In contrast to a missile, mortar or machine gun, many cyber weapons can replicate themselves, infecting third-party computers, and spreading much like a bioweapon agent.

Finally, there is the so-called **"attribution problem"**. In the cyber realm, it may be impossible to know for sure who was behind an incident. IP-addresses can be masked and the origin of an attack can be disguised. Even if the source of an incident or attack is traced back to a certain country, city or building, this would not necessarily give away the perpetrator. A malicious group from state A could, for example, attack state B using public WiFi in state C.

But this is not all. If attribution is problematic or even impossible, well-established military concepts like retaliation and deterrence cannot work, rendering old-fashioned military answers to stability problems obsolete. States have reacted in different ways to these **new challenges**.

In October **2012**, then US Secretary of Defense Leon Panetta publicly announced: "Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America". Whether this claim is well founded or a mere bluff is unclear, but potential attackers might be thinking twice now – surely his intent.

Today, attribution usually rests on the combination of tools including digital forensics and classical intelligence work. If, for example, a particular building has been identified as the source of a constant attack, old-fashioned observation kicks in.

One of the often-heard buzzwords in this context is **"autonomous hack-back"**. The idea is that an automated system which detects an intrusion attempt will follow the datastream back to its source and cause damage to the attackers system. While this has a high potential for sudden escalation, of course, it is often overlooked that a hackback only works if the institution hacking back has prior knowledge about the attacker's system.

The Cyber Kill Chain

The arms manufacturer Lockheed Martin has developed the concept of the "Cyber Kill Chain", a **model of how a cyberintrusion works**.

Today, there are many variants of the "kill chain" and we present a rather consolidated version here. What is important, however, is that the cyber kill chain dictates that for any form of counter attack in the case of an attack, the **defender needs prior knowledge** of the attacker's system. So even if a state has no intention of offensive cyberoperations, it has to actively look for weak spots in the computer systems of potential adversaries.

Reconnaissance and Weaponization

After careful reconnaissance of the potential victim, a "weaponized" file is created, aiming at a specific exploit. While looking harmless (e.g. .pdf, .mp4 or .jpg), the file contains malicious code.

Delivery and Exploitation
The file is delivered to the target (e.g. by a forged email) and run, thereby exploiting the preselected vulberability of the targeted system.

Privilege Escalatation
The malicious code installs a "beachhead" granting access to the system. From this beachhead, the intruder aims for privilege escalation, for example administrator instead of user rights.

Achieving Objectives
Finally, after gaining command and control the intruder can achieve his or her objective, be it data exfiltration, data destruction, data manipulation or simply switching off the system.

In a military context, for example, an intruder could place sleeping executable code in a system, reacting to specific circumstances.

Zero Day Exploits
Updates and patches will of course interrupt the kill chain, so intelligence agencies and military actors are always looking for new and unknown weak spots, so-called zero-day exploits.

There is a black market for zero day exploits which have been known to the general public. Complex cyber operations, like Stuxnet, are based on several zero-day exploits.

The Problems of Arms Control in Cyberspace

This video debates:

- why **arms control** is particularly difficult in the cyber realm
- what kind of **agreements** have been made so far
- whether **soft norms or legally binding treaties** should be aimed for
- whether **confidence building measures** could make a difference

One of the most important questions regarding cyber weapons has been whether – and if so, how – **arms control measures** can be applied in the cyber realm. According to many arms control experts, the "gold standard" of arms control usually entails, first, **a legally binding treaty**, second, **restricting a clearly and detailed defined subject** and, third, ensuring compliance through an effective yet non-intrusive **verification regime**. Unfortunately, it is significantly harder to archive this in cyberspace than in other more classical military realms.

First, it is hard for states to agree on what to regulate or ban to begin with. Well established arms control concepts like "effector" or "carrier" – introduced in learning unit one – are hard to apply. **Second**, given the fast pace of technological developments in information technology, detailed arms control agreements might always be behind current technological trends. **Third**, by their very nature, cyber weapons are basically nothing but software code and can be programmed, stored on or released from any computer or mobile device. In consequence, hiding malicious code or changing code on the fly is extremely easy. This means that verification in the arms control sense is a real challenge, and trust is way harder to archive.

Given these problems, **two other paths** are currently in the limelight: One is to focus on **voluntary normative restraints** rather than legally binding treaties, the other is to implement so-called **transparency and confidence building measures**, or CBMs. Both approaches have pros and cons.

CBMs offer transparency and information exchange on a voluntary basis but do not restrict actors in the way arms controllers would like. They are relatively **easy to achieve**. The OSCE member states, for instance, have agreed on certain CBMs to defuse emerging tensions, for example setting up official contact points. And in 2013, Russia and the United States established a cyber hotline to inform each other about relevant cyber instances.

In contrast to CBMs, normative restraints or simply **"norms"** "reflect the international community's expectations, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States", as the report of the 2015 UN Group of Governmental Experts explains.

The Russian Federation first suggested developing behavioural norms in a draft proposal to "regulate" "Information Warfare" and its subcomponent cyberwarfare in 1998. Russia tried to bind the technologically more advanced US to international norms, but with no result. Since then, however, some international norms on responsible state behaviour in the cyber realm seem to have emerged, like "do not allow your territory to be used for internationally wrongful acts using information technology" or "do not intentionally damage critical infrastructures".

Interestingly enough, not only states have acted as norm entrepreneurs, but also **private business** and **intelligence agencies**. But norms can be violated and the level of compliance is dependent on the internalization of the norm by all actors. Some experts, however, still think that at least some forms of harder arms control might be able to be applied to military cyber preparations and operations.

One approach could be a **binding international definition** of what constitutes a cyber weapon that is strongly tied to technical aspects and can be assessed before its actual usage. A second venture would be the establishment of technical approaches **to control or oversee military IT networks** to detect the application of weaponized code. None of these tools could prevent covert state activities (a burden that arms control has always had to carry) – but they can create important steps towards more effective cyber verification regimes.

Difficulties of Classical Arms Control in Cyberspace

What to control?
In a classical arms control agreement, participating parties exactly define what "effector" or "carrier" falls under the treaty. These terms are less clear in the cyber realm.

The Verification Problem
Solid verification is one of the important pillars of successful arms control agreements. However, how to verify complex software without being too intrusive is a problem yet to be solved. This also includes updates.

Different Classes of Actors
Traditionally, the relevant actors in arms control are nation states. Not much thought has been given to the question of how non-state actors can be included into formal arms control agreements.

The Rapid Technological Development
Even if the first problem, what to control, could be solved, the rapid technological development might render all agreements useless after a very short time.

The Attribution Problem
The attribution problem presented before makes it tricky or even impossible to identify breaches in case of attacks.

Scope
If a classical arms control agreement could be found, who should be a member? Should it only include the major cyber powers or should it be as universal as possible?

Treaties vs. Norms in the Cyber Realm

	Treaties	Norms
Positives	clearer understanding of do's and don'ts higher authenticity of forensic material - states still main actors in more dangerous forms of cyber-incidents	easier to achieve than treaties- involvement of actors beyond the state: "norm-entrepreneurs"- relevant legal basis has to be established as a norm anyway- ignorant to verification problems
Negatives	harder to achieve- problematic verification- take very long to negotiate- unrealistic, at least at the moment	violations hard to attribute ...- ... or no credible attribution- different interpretations possible- How deep is the internalization?- frustration when violated- no punishment for non-compliance

Assessment
- Norms seem achievable at the moment, treaties not so much.
- Who will be future norm-entrepreneurs? States? NGOs? Private Companies? Even intelligence agencies?
- Can norms be a the stepping stone towards legally binding treaties? At least when supported by (voluntary) Confidence Building Measures (CBMs)?

What Norms? Cybernorms and CBMs in the 2015 UN GGE Report

So far, the 2015 UN GGE report `[https://docs.un.org/en/A/70/174]` has been the last report unanimously accepted by all experts involved, focusing on relevant norms in the cyberrealm.

The report states:

> norms reflect the international community's expectations, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States"
> United Nations A/70/174, p.7

According to the 2015 UN GGE report, **states behaving responsibly** should:

- not allow "**their territory to be used** for internationally wrongful acts using ICTs" (p.8)
- "not conduct or support ICT activity that … intentionally damages **critical infrastructure**" (p.2)
- respect **human rights** on the internet and the **right to privacy** in the digital age (p.8)
- "increase **stability and security** in the use of ICTs" and prevent harmful practices (p.7)
- "**consider all relevant information**" in case of ICT incidents (p.7)
- "consider how best to cooperate to **exchange information**" (p.8)
- "**prosecute terrorist and criminal use of ICTs**" (p.8)
- "take appropriate measures to **protect their critical infrastructure**" (p.8)
- respond to "requests for **assistance**" by other states (p.8)
- "encourage responsible reporting of **ICT vulnerabilities** and share remedies" (p.8)

The 2015 report also contains **recommendations for voluntary confidence building measures**:

- identification of **"points of contact"** for cases of "serious ITC incidents" (p.9)
- development "of and support for bilateral, regional, subregional and multilateral **consultations**" (p.9)
- "Encouraging …. **transparency** at the bilateral, subregional, regional and multilateral levels" (p.9)
- provision of "**national views** of **categories of infrastructure that they consider critical** and national efforts to protect them" (p.9)
- additional "confidence-building measures that would strengthen **cooperation on a bilateral, subregional, regional and multilateral basis**" (p.9)

New Actors, New Interests, New Stakeholders?

Traditionally, norms regulating the field of information and telecommunications have been set by **state actors**. First initiatives were, for example, brought forward by Russia before the turn of the Millenium.

More recently, however, **new actors** have joined the field, for a variety of reasons. In a recent and widely cited publication by Illina Georgieva [https://pariscall.international/en/principles], the author argues that

> security and intelligence agencies have become major actors in the cybersecurity landscape
> Georgieva 2020: 33

Just with their actions, these agencies are setting norms for appropriate, or at least accepted behavior, for the international community, sometimes in conflict with other, more formal normative regulations.

Other actors which have become more active, and a cause for debate, have been **private companies**. Case in point is the so-called "Paris Call for Trust and Security in cyberspace" [https://pariscall.international/en/], a cybersecurity agreement promoted by, amongst others, Microsoft, Facebook or Google. The call features 9 essential principles.

According to a Microsoft blog, the support for the call "demonstrated a widespread, global, multi-stakeholder consensus about acceptable behavior in cyberspace." In contrast to these private companies, the US government refrained from endorsing the document.

It is obvious, however, that companies did not push the call for altruistic reasons, but because cyber incidents are a threat to their core business models.

Given their interest and often enormous resources, we will see the shift from lobbying their national governments to actually promoting an agreement together with foreign governments probably more often in the future.

Cyber-Related Agreements Throughout the Years

After a slow start in the 90s and early 2000s, international agreements between states regarding cyberspace have become more common in the last decade. These agreements have often been at the regional (or alliance) level with recent efforts to establish international norms across the entire international community. In most cases, the agreements simply reaffirm the position that international law should apply in cyberspace. The establishment and enforcement of cyber norms are still in the making. This timeline presents an overview of the various cyber-related agreements from the last two decades.

References

- Osula, Anna-Maria /Rõigas, Henry (2016): Introduction, in: Osula, Anna-Maria /Rõigas, Henry (eds), International Cyber Norms: Legal, Policy & Industry Perspectives, Tallinn: NATO CCD COE Publications, 11-22. View PDF [https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_full_book.pdf]
- Van Horenbeeck, Maarten (2018): "Cybersecurity Culture, Norms and Values: Background paper to the IGF Best Practices Forum on Cybersecurity." Internet Governance Forum 2018. View PDF [https://www.intgovforum.org/en/system/files/filedepot/13/igf_2018_-_bpf_on_cybersecurity_background_paper_-_culture_norms_and_values_0.pdf]

Data compiled by Jessica Draper

December 22, 1992 · International Telecommunication Union

The Constitution and Convention of the International Telecommunication Union [https://treaties.un.org/doc/Publication/UNTS/Volume%201825/volume-1825-I-31251-English.pdf] was the founding document of the International Telecommunication Union with the aim of "facilitating peaceful relations, international cooperation among peoples and economic and social development by means of efficient telecommunication services."

A provision of this treaty includes the International Telecommunications Regulations, first established in 1988, which outlines various principles related to the development and operation of telecommunication services. However, regulations referring to the malicious use of such services between states are not addressed.

November 23, 2001 · Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime [https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf], originating out of the Council of Europe, was the first international treaty to address crimes committed via computer networks, "dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security." Its main objective was to pursue a common criminal policy aimed at the protection of society against cybercrime. Sixty-four states have ratified the treaty, including the United States. Russia opposes it on grounds of sovereignty.

June 16, 2009 · Shanghai Cooperation Organization, Yekaterinburg Agreement
This "Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security" [https://treaties.un.org/doc/Publication/UNTS/Volume%202815/Part/volume-2815-I-49374.pdf] (Source [https://treaties.un.org/doc/Publication/UNTS/Volume%202815/Part/volume-2815-I-49374.pdf]) addressed the need among SCO members (China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan) to cooperate in curbing the development of cyber weapons and attacks. Defining concepts such as "information security" and "information war," it is the first international agreement to acknowledge and address issues of cyber warfare between states.

This agreement further formed the basis of the "Code of Conduct for Information Security" submitted to the UN in both 2011 and 2015, but it has not been put to a vote (Osula and Rõigas 2016).

December 14, 2012 · International Telecommunication Regulations (ITRs)
The Final Acts of the World Conference on International Telecommunications [https://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf] is a renegotiation of the 1988 ITRs. The International Telecommunications Union said the document would help countries coordinate efforts against spam and increase the development and availability of serivces around the world. However, the question of state governance over the development of the internet's technical infrastructure was hotly debated. As a result, only 89 states signed the treaty, excluding many Western democracies such as the US, Canada, the UK, and Australia (BBC, 2012 [https://www.bbc.com/news/technology-20717774]).

June 17, 2013 · Bilateral Agreement Between the US and Russia
This bilateral agreement between the US and Russia aimed to "[extend] traditional transparency and confidence-building measures to reduce the mutual danger" both states face from cyber threats. In this effort, it created a working group that assesses emerging cyber threats and proposes joint measures to address them, as well as a hotline to share information regarding these matters.

June 24, 2013 · UN Group of Government Experts (2013)
The 2013 Group of Governmental Experts on Developments in the Field of Information and Telecommunications the Context of International Security included 15 countries agreeing that international law, such as the UN Charter, is the main source for regulating offensive state behaviour in cyberspace. In seeking to establish norms derived from international law, the document stated, "although the work of the international community to address this challenge to international peace and security is at an early stage, a number of measures concerning norms, rules and principles for responsible State behaviour can be identified for further consideration."

December 3, 2013 · OSCE Confidence-Building Measures
Member states of the OSCE agreed to confidence-building measures [https://www.osce.org/files/f/documents/d/1/109168.pdf] aimed at reducing the risk of conflict stemming from the use of information and communication technologies (ICTs). Largely focused on information sharing, these measures sought to "enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs."

July 17, 2014 · The 6th BRICS Summit: Fortaleza Declaration
As part of the Fortaleza Declaration [http://www.brics.utoronto.ca/docs/140715-leaders.html] at the 6th BRICS Summit, Brazil, Russia, India, China, and South Africa agreed to "explore cooperation on combating cybercrimes" as well as to "recommit to the negotiation of a universal legally binding instrument in that field."

September 5, 2014 · NATO Wales Summit Declaration
In their Wales Summit Declaration [https://www.nato.int/cps/en/natohq/official_texts_112964.htm], NATO member states endorsed an "Enhanced Cyber Defence Policy" that reaffirms a cyber defense responsibility of the alliance and "recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace." The declaration also established cyber defense as "part of NATO's core task of collective defence."

February 11, 2015 · Council of the European Union on Cyber Diplomacy
In the Council Conclusions on Cyber Diplomacy [https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf], European Union member states are encouraged to work towards a global understanding of "how to apply existing international law in cyberspace and to the development of norms for responsible state behaviour in cyberspace." States are further encouraged to "strongly uphold the principles regarding State responsibility for internationally wrongful acts and to take the initiatives necessary…to ensure that they are fully respected and enforced in cyberspace."

While it reitereates the position that existing international law is applicable in cyberspace, it also discusses internet governance, promotion and protection of human rights in cyberspace, and other capacity-building and engagement topics.

May 8, 2015 · Bilateral Agreement Between China and Russia
China and Russia "signed a memorandum not to launch hacking attacks against each other and condemned efforts to destabilize internal politics via the Internet" (New York Times, 2015 [https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html]). While "perhaps 70 percent" of the agreement had been borrowed from the previous agreement under the Shanghai Cooperation Organization, this agreement added "language protecting internal sovereignty in cyberspace."

July 22, 2015 · UN Group of Government Experts (2015)
As a second iteration of the original 2013 GGE report, this 2015 report from the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security [https://docs.un.org/A/70/174] sought to "outline additional points of agreement and to further develop the content of the 2013 report" (Osula and Rõigas 2016). The report expands the discussion of norms and recommends that states "cooperate to prevent harmful ICT practices and should not knowingly allow their territory to be used for internationally wrongful acts using ICT." States such as the United States, Russia, and China were included in this report.

September 26, 2015 · Bilateral Agreement Between the US and China
The US and China agreed to cooperate on matters of cybercrime investigations. Both states also support the GGE reports on norms of behavior and other crucial issues for international security in cyberspace. In addition, the agreement created a hotline for direct communication of information requests regarding malicious cyber activity.

November 16, 2015 · G20 Leaders' Antalya Communiqué
In their Antalya Summit Communiqué [https://www.consilium.europa.eu/media/23729/g20-antalya-leaders-summit-communique.pdf], G20 members welcomed the 2015 GGE report affirming that international law, in particular the UN Charter, is applicable to state conduct in cyberspace. They also committed themselves to the view that all states should abide by norms of responsibile behavior and should "promote security, stability, and economic ties with other nations" within cyberspace.

November 21, 2017 · Call to Protect the Public Core of the Internet
As a multistakeholder commission, the Global Commission on the Stability of Cyberspace (GCSC) urged all stakeholders within government, industry, technical and civil society to adhere to the following norm proposal [https://cyberstability.org/research/call-to-protect.html]:

"Without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace."

Here, "public core" refers to packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, and physical transmission media.

April 28, 2018 · ASEAN Leaders' Statement on Cyber Security Cooperation
At the 32nd Association of Southeast Asian Nations Summit, ASEAN leaders addressed in a statement [https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf] the threats existing in cyberspace and reaffirmed the position that international law applies in the cyber environment. The statement acknowloedged that "the promotion of international voluntary cyber norms of responsible State behaviour is important for cultivating trust and confidence and the eventual development of a rules-based cyberspace." ASEAN member states agreed to improve coordination of cybersecurity policy development and capacity building initiatives towards this end.

May 28, 2018 · Call to Protect the Electoral Infrastructure

The GCSC proposed another norm regarding electoral infrastructure [https://hcss.nl/wp-content/uploads/2022/08/GCSC-Call-to-Protect-Electoral-Infrastructure.pdf]:

"State and non-state actors should not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites."

November 2018 · GCSC Norm Package

The Global Commission on the Stability of Cyberspace further introduced a "norm package" of additional norms that state and non-state actors should abide by. These norms include:

- Norm to Avoid Tampering
- Norm Against Commandeering of ICT Devices into Botnets
- Norm for States to Create a Vulnerability Equities Process
- Norm to Reduce and Mitigate Significant Vulnerabilities
- Norm on Basic Cyber Hygiene as Foundational Defense
- Norm Against Offensive Cyber Operations by Non-State Actors

December 11, 2018 · Paris Call for Trust and Security in Cyberspace

With support of 67 States, 139 international and civil society organizations, and 358 entities of the private sector, the Paris Call [https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433-1.pdf] reaffirms that "international law, including the United Nations Charter in its entirety, international humanitarian law and customary international law is applicable to the use of information and communication technologies (ICT) by States." The delcaration also condemns the use of malicious cyber activities in peacetime and welcomes the protection of critical infrastructure that are vulnerable to such activities. Further, it supports cooperation to prevent malicious cyber activity (including undermining electoral processes, theft of information for providing competitive advantages, etc.) and encourages the strengthening of defence and security against such actions.

The US, China, and Russia did not sign the declaration. However, American technology corporations such as Microsoft, Facebook, Google, IBM, and HP all endorsed the agreement.

4. Offence and Defence of Major Cyber Powers

How To Watch and Read This Chapter

The **main objective** of this chapter is to make you understand what it means for a country to be cyber capable and to give you an overview of major powers' cyber defence and offence strategies.

In the former two chapters, we covered concepts and definition of cyber war and how cyber conflict relates to international law. With this foundation, we can now move on to outline the **cyber defence strategies of major cyber international powers**, and show how cyber operations are often intertwined with broader information warfare strategies.

To do this, this chapter provides, first, a **framework to analyse countries' cyber capabilities** through the taxonomy developed by the International Institute for Strategic Studies, **IISS**, in London.

Second, the chapter gives **an overview of the cyber policies** of two Western countries, namely the United Kingdom and the United States. An example of the evolution of Western strategic thinking in cyberspace are the UK **"Active Cyber Defence"** and the US **"Persistent Engagement"** policies. This section will also explore the role of and efforts by NATO and how national strategies are linked to the development of **NATO's Cyber Defence Policy**.

Third, this chapter presents two other major players in cyberspace, **Russia** and **China**, and their modus operandi in this environment. This section will uncover how China uses cyberspace to advance its strategic objectives and how Russia devised an offensive cyber policy leading to destabilization in the West. It also unveils how these countries' cyber operations are part of a broader information strategy designed to weaken adversaries while keeping the level of conflict below the threshold that would trigger a direct military confrontation.

In sum, we will see that cyber operations have become an important part in the power-play of great powers.

Cyber Military Capabilities: Which Countries Have Offensive or Defensive Doctrines?

This map shows the countries that have issued a **cyber security military doctrine**. Cyber military strategies typically explain governments' views on issues such as offensive and defensive cyber operations and norms of behaviour in cyber space, among other things. They are usually produced by countries' ministries of defence.

This map is based on the Global Cyber Strategies Index developed by the Center for Strategic and International Studies.

The Index also includes a list of existing cyber strategies and laws by country and includes civilian and military cyber defence, digital content, privacy, critical infrastructures, e-commerce and cyber crime policies and regulatory frameworks.

Measuring Cyber Defence Capabilities: the Methodology of the IISS I

For the first time in their 2020 edition of the Military Balance `[https://www.tandfonline.com/toc/tmib20/120/1]`, the International Institute for Strategic Studies (IISS) has systematically outlined the **significant factors** that are useful to understand the **cyber military capabilities** of a country.

The Institute developed a **taxonomy** that focuses on **enablers and indicators**. These are derived from both the civilian sector and the armed forces (see learning unit 12 `[/lu-12/]`) and, because of that, the IISS notes the assessment of capabilities is more challenging as the lines between military and civilian capabilities, assets and operations are often blurred.

As of now, the IISS has made available only the taxonomy of cyber defence capabilities. In the near future, the institute will make available **national case studies** that will highlight national cyber military capabilities.

The Military Balance
Tylor and Francis/International Institute Strategic Studies (IISS) - The Military Balance 2020. Copyright © The International Institute for Strategic Studies. Reprinted by permission of Taylor & Francis Ltd, http://www.tandfonline.com on behalf of The International Institute for Strategic Studies

The IISS's taxonomy is a useful **analytical framework** that puts in perspective what it means to have "cyber power" in the military realm and to draw comparisons among countries.

The next slide shows all **enablers and indicators** that make up a country's cyber capability.

The main enablers are:

- strategy and doctrine
- command and control
- cyber empowerment and dependence
- cyber security and resilience
- global leadership in cyberspace
- military capability for cyber coercion

Measuring Cyber Defence Capabilities: the Methodology of the IISS II

Military Strategy/Doctrine – command and Control and Integration

- cyber defence related documents
- national- and command-level formations
- integrating bodies, such as national-security councils
- military cyber intelligence capacity

Protection and Resilience of Military Networks

- automated joint-force cyber situational-awareness system; military computer emergency response teams (MIL CERTs)
- military cybersecurity exercises

Military Capacity for Cyber Coercion

- decision-making framework
- recent reported used of cyber military forces

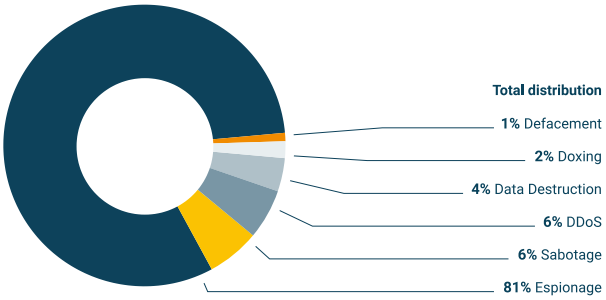
Military Research and Development and Human Capacity

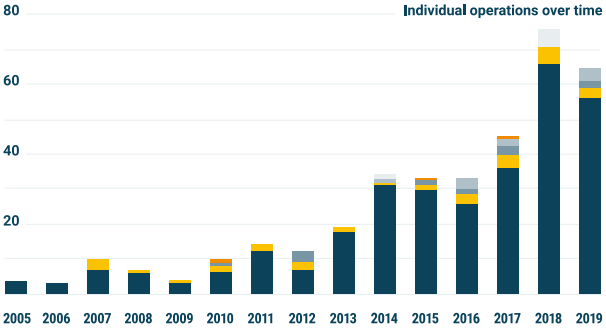
- research institutes (governments and military affiliated)
- military exercises in cyber defence or offensive actions
- active recruitment

Extent of a Military Force's Digital Dependence/ Enabling

- space-based intelligence, ISTAR capability
- global operations and therefore reliance on global communications capabilities
- significant investments in digitally enabled technology
- ability to independently access and manoeuvre in space

Tracking State-Sponsored Cyber Incidents





Distribution of Cyber Operations (total, over time)
Cyber Operations Tracker, own calculations

The Cyber Operations Tracker `[https://www.cfr.org/cyber-operations/]` of the Council on Foreign Relations (CFR) is a database of the publicly known state-sponsored incidents that have occurred since 2005.

The tracker includes only attacks that are perpetrated by a nation state or an entity that is affiliated with a nation state.

It includes **6 types of operations**: DDoS, espionage, defacement, data destruction, sabotage and doxing.

The main takeaways so far:

- 28 countries have been suspected of launching cyber operations.
- Countries have reacted by imposing sanctions and using indictments.
- State-sponsored cyber operations have caused power outages; as in Ukraine in 2015 and 2016.

The Cyber Defence Policy of Selected Major Players: The US and the UK

These videos explain:

- the **United States cyber defence policy**, including the new concept of "Persistent Engagement"
- the **United Kingdom cyber security policy**, including new data on the "Active Cyber Defence" programme

Let us first look at the most important international actor, the **United States of America**. The United States' Department of Defense released its **new cyber strategy** in 2018, which superseded the three-year-old version from 2015. The new strategy has **five main objectives**:

"**Ensuring** the Joint Force can achieve its missions in a contested cyberspace environment; **Strengthening** the Joint Force by conducting cyberspace operations that enhance US military advantages; **Defending** US critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident; **Securing** DoD information and systems against malicious cyber activity, including DoD information and non-DoD-owned networks; **Expanding** DoD cyber cooperation with interagency, industry, and international partners."

Despite the document being 3 years newer than the previous version, these objectives did not necessarily overhaul US military policy in cyberspace. Instead, the novelty of the document resides in the introduction of the concept of "persistent engagement".

In contrast to the milder tones of the previous version, the document openly admits the US is in a long-term struggle with Iran and North Korea, but most notably China and Russia.

"We are engaged in a long-term strategic **competition with China and Russia**. These States have expanded that competition to include persistent campaigns in and through cyberspace that pose long-term strategic risk to the Nation as well as to our allies and partners. **[…]** Our focus will be on the States that can pose strategic threats to US prosperity and security, particularly China and Russia."

The document states that because these actors are deterred to conventionally engage against the US, they are resorting to cyber instruments to challenge democratic processes or threaten critical infrastructures.

To confront this, the strategy argues that the **US Cyber Command** should be engaged in a **day-to-day competition**, what the new strategy refers to as "persistent engagement." In this daily struggle, the US will work to collect intelligence, prepare capabilities and **defend forward**. In other words, it will attempt to disrupt foreign operations at its origins. These will also include all those operations that fall below the threshold of conflict, which is the usual environment where militaries are engaged.

"We will defend forward to **disrupt or halt malicious cyber activity** at its source, including activity that falls below the level of armed conflict **[….]** The Joint Force will employ offensive cyber capabilities and innovative concepts that allow for the use of cyberspace operations across the full spectrum of conflict."

Some analysts believe that the new strategic posture does not make US policy offensive or escalatory in nature and make the example of "malware inoculation." When the US Cyber Command goes on a hunt in an adversary's cyberspace and discover malign malware, they cooperate with other US departments and agencies by **exposing the malware** and make it public through **information sharing platforms** such as VirusTotal. Exposing the malware allow cyber defenders to patch vulnerabilities and increase resilience at home. Hence, malware inoculation does not involve disruptive cyber operations, but it is based on information sharing.

Other analysts, instead, think that a strategy of persistence presence might lead to mistakes, misperceptions, miscalculations and could also strategically fail if the US are unable to play the game hard enough to apply negative feedback.

In sum, the new document signals an important change in US cyber defence policy, an approach which is in stark contrast with UK one, the topic of discussion of our next episode.

In the last episode, we looked at the US cyber strategy more closely. The approach developed by the **UK government** is fairly different. It is called **"active cyber defence"** (ACD) and it is outlined in the "National Cyber Security Strategy 2016–2021", published in November **2016**. The overall aim is to focus on those measures helping to strengthen a network or make a system more robust. In particular, the **objectives of this approach** are to:

- make the UK a much **harder target**
- **block malware communications** between victims and attackers
- **secure internet traffic** from malicious actors' hijacking
- harden UK **critical infrastructures**
- **disrupt** the business model of attackers

To achieve these objectives, the UK government aims to work with the industry – especially **communication service providers** – to block malware attacks and prevent phishing activities that rely on domain spoofing. This will be done by deploying an **email verification system**. It will also scale up programmes within the **Government Communications Headquarters** (the GCHQ), the **Ministry of Defence**, the MoD, and the **National Crime Agency**, NCA, to disrupt malicious activities and promote security best practices through multi-stakeholder organizations such as the **Internet Corporation for Assigned Names and Numbers** (ICANN) and the **UN Internet Governance Forum** (IGF).

According to government data, since its launch Active Cyber Defence has reduced the UK's share of visible global phishing attacks by more than half (from 5.3% to 2.4%) and removed nearly 140,000 phishing sites hosted in the UK between September 2017 and August 2018.

According to analysts, the ACD programme has so far succeeded in reducing the incidence and the effect of low-level cybercrime and these measures should be extended beyond the public sector. Moreover, this **defensive approach** can be exported to likeminded countries that have a different approach from hacking back or other more escalatory policies.

Finally, if the ACD can effectively and efficiently operate and provide benefits at a low direct cost for citizens it may even be considered a public good.

The Role of NATO

Allies are responsible to protect their own networks and systems, but **NATO supports** them by:

- sharing real time information
- deploying rapid-reaction cyber defence teams
- developing common targets to strengthen cyber capabilities
- organizing exercises such as Cyber Coalition

One important actor is the **NATO Communications and Information Agency** (NCIA) which provides cyber security services throughout NATO, including by handling and reporting incidents through its **NCIRC Technical Centre** in Belgium. It has a team of 200 experts.

In 2023, the new **Cyber Operations Centre** will be operational. Its tasks will include providing situational awareness to inform operations and coordinating the Alliance's operations in cyberspace.

NATO argues:

> NATO and its Allies rely on strong and resilient cyber defences to fulfil the Alliance's core tasks of collective defence, crisis management and cooperative security. The Alliance needs to be prepared to defend its networks and operations against the growing sophistication of the cyber threats and attacks it faces"
>
> [nato.int](https://www.nato.int/cps/en/natohq/topics_78170.htm)

NATO has also defined its own **Cyber Defense Policy** which has been evolving since 2008.

The next slide gives an overview of NATO guiding principles in cyberspace, a chronology of the policy evolution as well as the main actors involved in the Alliance's cyber decision-making.

NATO Cyber Defence Policy

Main Principles

- **Cyber defence** is part of NATO's core task of collective defence.
- NATO affirmed that **international law** applies in cyberspace.
- NATO recognises that Allies stand to benefit from a **norms-based**, predictable and secure cyberspace.
- NATO's main focus in cyber defence is to **protect its own networks** (including operations and missions) and **enhance resilience** across the Alliance.
- NATO reinforces its capabilities for **cyber education**, training and exercises.
- Allies are committed to enhancing **information-sharing** and **mutual assistance** in preventing, mitigating and recovering from cyberattacks.

For details, study main principles on nato.int website `[https://www.nato.int/cps/en/natohq/topics_78170.htm]`

Policy Evolution

- **2008**: NATO approves first cyber policy
- **2011**: NATO approves second cyber policy
- **2014**: Wales Summit: new cyber policy and action plan
- **2016**: Warsaw Summit: NATO recognizes cyber space as a domain of operation and Cyber Defence Pledge
- **2017**: updated Cyber Defence Action Plan
- **2018**: Brussels Summit: new Cyberspace Operations Centre
- **2019**: new NATO guide setting out a number of tools for responding to cyber attacks

Main Actors

- **North Atlantic Council** provides high-level political guidance
- **Cyber Defence Committee** is the lead committee for political governance and cyber defence policy in general
- **NATO Cyber Defence Management Board** is responsible for coordinating cyber defence throughout NATO civilian and military bodies
- **NATO Consultation, Control and Command Board** consults on technical and implementation aspects of cyber defence
- **NATO Military Authorities** (NMA) and the **NATO Communications and Information Agency** (NCIA) identify operational requirements, acquisition,

implementation and operating of NATO's cyber defence capabilities

The Cyber Capabilities of Russia and China

Russia
Russia has been investing significantly in developing tactics and tools to strengthen its cyber arsenal. According to some estimates, the Kremlin invests $300 million per year and has a dedicated 1,000 strong cyber army [https://www.newamerica.org/cybersecurity-initiative/reports/russia-china-cyber-offensive-latam-caribbean/].

Russian intelligence has been integrating network with information operations.

Russia has used cyberspace to:

- prepare for military kinetic operations
- engage in direct cyber operations as in Ukraine
- enable influence operations

China
China's cyber capabilities and skills are comparable to those of Russia. China uses cyber capabilities in both peace and wartime to enhance its overall strategic objectives. Cyber is incorporated in the Diplomacy Information Military and Economic (DIME) operation spectrum.

China has used cyberspace to:

- advance diplomatic claims
- improve its own international perception
- bolster military capabilities
- advance economic interest

Cyber Operations as a Tool in Influence Operations? Similarities and Differences in Russian and Chinese Approaches

Differences: Russia
- **Geopolitics**: Russia is economically declining and aims at reversing the current international system.
- **Ethos**: Russia cares less about its international reputation.
- **Targets**: Russia targets the general population in deeply divided and polarized societies.
- **Narrative**: Russia supports the message of a declining, weak and divided West, discrediting its enemies.

Therefore, **Russia employs more aggressive techniques in the information environment**.

Similarities
- Influence and information operations are "business as usual" in the conduct of domestic and foreign policy.
- Information operations are used domestically, albeit in two different ways: in Russia to manipulate, in China to censor.
- There is some degree of dysfunctionality in the administration and implementation of information and influence operations.
- China is adopting some techniques from Russian playbook in Taiwan and Hong Kong: it is using cross platforms and coordinated networks of fake and automated accounts to amplify its messages and with the overall goal to generate favourable offline effects.

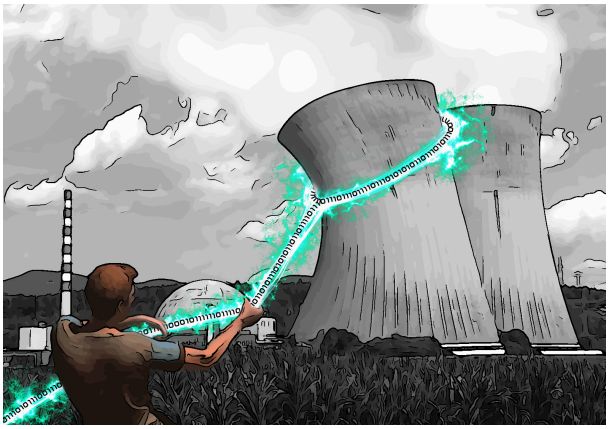
Differences: China
- **Geopolitics**: China is an emerging global power aiming at shaping the world with its own norms.
- **Ethos**: China wants to portray itself as a good global citizen.
- **Targets**: China mainly targets the "overseas Chinese community".
- **Narrative**: China wants to promote the idea of a great, but non-threatening, China.

Therefore, **China is considered less risk averse in cyber operations** and does not engage in hack-and-leak operations like the Russian kompromat.

Quiz

View quiz at https://eunpdc-elearning.netlify.app/lu-19/

5. Cyber Terrorism and the Protection of Critical National Infrastructures



Aspects of Cyber Conflict (pt. 4)
Linda Graf, https://cltc.berkeley.edu/cybervisuals/ (CC BY 4.0)

How to Watch and Read this Chapter

The **main objective** of this chapter is to give you an overview of the current threat posed by "cyber terrorists" to Critical National Infrastructures (CNI) and what measures can be put in place to mitigate their actions.

In the last chapter, we looked at state actors. This chapter now provides an **overview of cyber terrorism** and evaluates whether cyberterrorists pose a threat to critical national infrastructures, CNI.

First, as the concept of terrorism is not universally accepted, we attempt to provide a working definition for the purpose of this overview.

Second, in this chapter we consider the goals and tactics of major terrorist organizations employing Information Communication Technology to advance their goals, namely ISIL/Da'esh and al-Qaeda. It also assesses whether it would be possible for cyber terrorists to mount an effective online operation to dislocate Western critical national infrastructures. It points out that there is little evidence that terrorist organizations have the technological resources and the intellectual skills to deploy Stuxnet-like attacks.

Finally, this chapter offers an example of what kind of operations can be used to curb online terrorism in the context of a military operation. To get deeper into the operational aspect, it uses as a case study "Operation Glowing Symphony," which was conducted by the US Cyber Command to disrupt ISIL network operations.

Cyber Terrorism: a Working Definition

To date, there are no universally accepted definitions of cyber terrorism, as the concept of terrorism in itself is highly disputed at the international level. For example a rebel group targeting police forces in the context of an escalating civil conflict might be labelled as a "terrorist group" or a "liberation army" depending on the stakeholder's perspective in the conflict.

There are however some **dictionary definitions**:

Merriam Webster [https://www.merriam-webster.com/dictionary/cyberterrorism] defines cyber terrorism as: "terrorist activities intended to damage or disrupt vital computer systems".

Similarly, the Cambridge Dictionary [https://dictionary.cambridge.org/dictionary/english/cyberterrorism] defines it as: "the use of the internet to damage or destroy computer systems for political or other reasons".

There are also **more elaborate definitions** as the one put forward by Luiijf, 2014 [https://doi.org/10.1016/B978-0-12-800743-3.00002-5], where the author considers relevant:

"The use, making preparations for, or threat of action designed to cause a social order change, to create a climate of fear or intimidation …"

made with the intention to achieve any goal (political, religious, racial)

"… by affecting the integrity, confidentiality, and/or availability of information, information systems and networks, or by unauthorized actions …"

which should involve violence, serious injuries, damage to properties, risk to health and a serious breach of the social and political stability and cohesion of a country.

This chapter uses the definition as proposed by the National Conference of State Legislatures [https://web.archive.org/web/20030110120948/http:/www.ncsl.org/programs/lis/CIP/cyberterrorism.htm]:

> The use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically."

Rather than defining the **act** this definition has the merit to restrict the concept of cyber terrorism to the **actors** (i.e. terrorist groups and individuals) who perform online actions to reach their goals.

This allows to achieve better conceptual clarity as a list of individuals and entities associated with terrorist activities

[https://www.un.org/securitycouncil/sanctions/information] is updated by the United Nations.

Terrorist Groups Using ICT: The Major Players

This video explains the strategic goals and tactics of major terrorist groups using ICT, including:

- **ISIL (Da'esh)**
- **al-Qaeda**

The **Islamic State of Iraq and Syria (ISIL/Da'esh)** is a terrorist organization that gained global prominence in 2014 with the occupation of large swaths of territories in Iraq and Syria. After a military campaign led by an international coalition, ISIL lost most of its territory and only held 2% of what it used to occupy by December 2017. In October 2019, the prominent ISIL leader Abu Bakr al-Baghdadi killed himself during a raid conducted by US special forces.

After territorial control declined, the terrorist organization outsourced their online activities and started to rely on specialized groups, **forming an online cyber terrorist network**. These are the organizations that are known to have been involved in supporting ISIL operations online.

These organizations have had different roles. For example, Cyber Caliphate Army, Islamic State Hacking Division, Islamic Cyber Army and most recently United Cyber Caliphate have been **hijacking or defacing websites** and social media accounts; they have also **disrupted systems and networks** of ordinary people and businesses and have used cyberspace to **spread ISIL's propaganda**. Other groups have supplied ISIL with **technical support** and **provided training** to adepts willing to join.

Despite the killing of its historical leader Osama Bin Laden in May 2011, **al-Qaeda** still has an online presence through three main components: the al-Qaeda Alliance Online, Youni Tsoulis (an e-jihadist), and the al-Qaeda Electronic. Al-Qaeda has been using cyberspace similarly to ISIL: to **spread jihadist literature**, to **create fundraising campaigns**, to use social media and **spread propaganda**, to incite to violence, to **deliver military training** to carry out violent attacks, to **glorify martyrdom** and the sacrifices of Islamic combatants and finally to **provide instructions** on computer security measures. One specific example of al-Qaeda online activities has been the publication of the English-periodical Inspire, which has been publicly exposing and spreading the organization's viewpoints. In terms of more specific disruptive capabilities, the al-Qaeda online network has allegedly been responsible for web defacements, DoS attacks, minor data breaches and the establishment and promotion of online forums where to learn how to hack.

But despite all these efforts and groups one question remains: Do terrorist groups pose a threat to critical national infrastructures? We will debate this on the following page.

Assessing the Evidence: Is There a Threat to CNI Posed By Terrorist Groups?

A study by Gross, Canetti and Vashdi (2017) [https://academic.oup.com/cybersecurity/article/3/1/49/2999135] has shown that exposure (in the form of video clips) to lethal and non-lethal cyber terrorism generate a "stress-based cyber terrorism effect".

Exposure to cyber terrorism is not harmless and leads to reactions similar to conventional terrorism, such as:

- stress
- anxiety
- insecurity, a preference for security over liberty
- a re-evaluation of confidence in public institutions
- a heightened perception of risk and support for forceful government policies

This leads into support for internet surveillance, regulation of the internet and kinetic responses to terrorism.

However, what is the current assessment of the threat posed by cyber terrorists?

According to the Worldwide Threat Assessment of the US Intelligence Community:

> Terrorists could obtain and disclose compromising or personally identifiable information through cyber operations, and they may use such disclosures to coerce, extort, or to inspire and enable physical attacks against their victims. Terrorist groups could cause some disruptive effects—defacing websites or executing denial-of-service attacks against poorly protected networks—with little to no warning."
>
> p. 6

Generally speaking, there is a **consensus among experts that terrorist groups' ability to launch major and large scale cyber attacks is lower compared to that of state actors**.

There are **two main reasons** for this assessment:

- Terrorists seem unable to develop new malware. Rather, they resort to what is already available.
- Perpetrating a major attack against a CNI would require not only advanced network operations skills, but also engineering expertise. These forms of expertise and skills could be hard to assemble for terrorist organizations.

However, because of the fast changes in technology and the possibility to acquire complex exploits from more sophisticated actors, cyber terrorists need continuous monitoring.

Tackling Terrorism Online: How the US Cyber Command Disrupted the ISIL Online Network

In the context of the international military intervention against the Islamic State of Iraq and the Levant (ISIL), the US military launched a cyber operation to dismantle the terrorist organization's ability to operate in cyberspace.

The task assigned to task force **JTF-ARES** was to curb ISIL activities in cyberspace. Instead, **Operation Glowing Symphony** tried to curb ISIL social media and internet propaganda.

Today, it is unknown whether Glowing Symphony is still ongoing, although it is known that JTF-ARES still operates.

Glowing Symphony and JTF-ARES activities are seen as a demonstration of the nation's offensive cyber capability and a model describing the "American way" of conducting cyber warfare [https://www.atlanticcouncil.org/blogs/new-atlanticist/the-american-way-of-cyber-warfare-and-the-case-of-isis/].

View interactive component at https://eunpdc-elearning.netlify.app/lu-19/

Operation Glowing Symphony: An Assessment

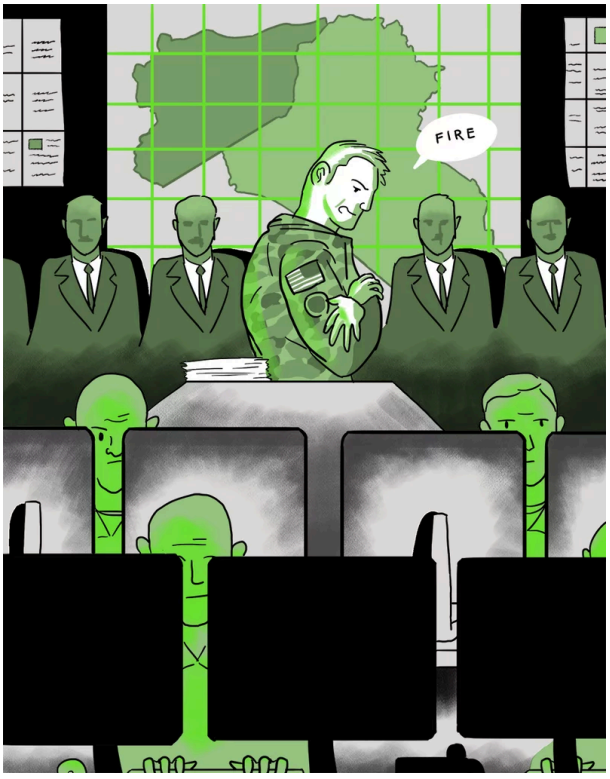
The National Security Archive [https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony] (NAS) obtained documents assessing the first phase of Operation Glowing Symphony.

Outcome of the operation:

- The operation is assessed to have "imposed time and resource costs" by disrupting activities, leading USCYBERCOM to assess "that OGS successfully contested ISIL in the information domain."

However **challenges** were also highlighted:

- shortcomings in **data exploitation capabilities**, mostly related to storage of the data itself
- problems in **targeting procedures** (clearing targets for engagement)
- **coordination** with other US agencies and departments



Josh Kramer / NPR, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis

Quiz

View quiz at https://eunpdc-elearning.netlify.app/lu-19/

6. The European Union's Role in Cybersecurity

The European Commission, https://digital-strategy.ec.europa.eu/en/library/eu-cybersecurity-act-glance

How to Watch and Read this Chapter

The **main objective** of this chapter is to give you an overview of the main institutional actors that have a role in the formulation and implementation of EU cyber security mission as well as an advanced understanding of the Union's cyber security policies.

Before, we talked about major actors, like the US, China or Russia, as well as NATO. Now we will shift our perspective to the **European Union**. In this chapter, we outline **EU policies in cyber space** with a particular reference to its foreign, security and defence measures.

First, we provide an overview of the policy and institutional framework in which EU cyber security takes place. This section describes the purpose of EU cyber policies and how these have evolved since the first strategy in 2013. This section also describes the main EU actors with a role in cyber security, namely the "policymaking" and the "policy-support" institutions and agencies.

Second, we delve more deeply into EU cyber foreign, security and defence policies, which are mainly designed and implemented by three actors, namely the European Commission, the European External Action Service and the European Defence Agency, as well as member states. We firstly introduce cyber diplomacy measures that are aimed at deterring malicious actors by imposing countermeasures as well as actions that have sought to establish a rule-based cyber space environment.

Finally, we look at EU cyber defence policy and the ties with NATO, another institution with a fundamental role in European cyber defence.

Cyber Security in the EU: Policy and Institutional Framework

In this video lecture, you will learn about:

- the **main "foundational" policies** of the European Union in the digital and cyber security field
- the **main institutions and organizations** with a prominent role in the making and execution of EU digital and cyber security policies

The European Union cyber security policy gained prominence in 2013 after the release of its first cyber security strategy **"An Open, Safe and Secure Cyberspace."** There, the EU vowed to achieve **five main objectives**. I quote:

- achieving **cyber resilience**
- drastically **reducing cybercrime**
- **developing cyber defence policy** and capabilities related to the Common Security and Defence Policy (CSDP)
- develop the **industrial and technological resources** for cyber security
- establish a coherent **international cyberspace policy** for the European Union and promote core EU values

In light of the changing threat and technological landscape, as well as mixed progresses in its implementation, the strategy was renewed in 2017 with the EU Cybersecurity Package. In December **2020**, the EU released a **new cyber security strategy**, which contains interesting new features:

- an EU-wide **Cyber Shield** composed of Security Operations Centres that use AI and machine learning to detect early signals of imminent cyber attacks
- a **Joint Cyber Unit**, with the aim of bringing together the various cyber security communities for the purpose of collecting information and implementing swift responses to cyber threats
- European solutions for strengthening internet security globally, including a public EU **DNS Resolver Service**
- a **Programme of Action in the United Nations** to address international security in cyberspace

According to the **ENISA's institutional map**, there are 22 actors that have a role in cyber security policy making, support and implementation in the EU. However, here we focus on those actors with a more pronounced role.

- Within the European Commission, several Directorates-General play an important role in developing cyber security, but the most central one is the DG for Communications Networks, Content

and Technology **(DG CONNECT)**. It has competences in areas such as network and information security, 5G and electoral security.
- Within the European Council, the **Horizontal Working Party on Cyber Issues** was established in 2016. It gathers member states' cyber ambassadors to discuss cyber security issues at the Council level.
- Within the European Parliament, the **Committee on Industry, Research And Energy** (ITRE) is the committee responsible for all discussions surrounding important EU-wide cyber security legislation. This includes, for example, the Network and Information Directive and the Cybersecurity Act.
- Finally the **European External Action Service**, the diplomatic service of the European Union, has an important role in promoting EU cyber diplomacy and in countering foreign disinformation.

When it comes to policy support and implementation, an important role is played by several actors:

- First, the **European Defence Agency**, EDA, which is the intergovernmental agency of the Council of the European Union devoted to defence issues. In the cyber realm, it is active in cyber defence capability development and in research and technology.
- Second, **ENISA**, which has tasks in areas such as the improvement of member states' cybersecurity capabilities, the development of common responses to large-scale cross-border attacks and, since 2019, drawing up cybersecurity certification schemes.
- Finally, there is **EUROPOL**, and in particular the European Cybercrime Center (EC3), which has the lead in providing a law enforcement response to cybercrime.

The NIS Directive and the Cyber Security Act

The Directive on security of network and information systems (the NIS Directive [https://digital-strategy.ec.europa.eu/en/policies/nis-transposition]) entered into force in August 2016 with the aim to increase the overall level of cybersecurity across the EU.

The main provisions of the directive are:

- identification of **operators of essential services** (i.e critical infrastructures)
- adoption of **cyber security national strategies**
- designation of **national competent authorities** and single point of contact
- establishment of Computer Security Incident Response Teams (**CSIRT**s)
- creation of the **Cooperation Group** among member states, ENISA and the Commission;
- Establishment of the EU CSIRTs network
- **security requirements and incident notification** for digital service providers

The Regulation on ENISA and on information and communications technology cybersecurity certification **(the Cyber Security Act)** came into force in June 2019. The regulation …

- … gave a **new mandate to ENISA**, the EU agency for cyber security. The Agency was granted a permanent mandate and was given new tasks. In particular ENISA will have a key role in the establishment of a cyber security certification framework and in enhancing operational cooperation in the EU in the wake of EU-wide cyber security attacks.
- … introduced a cyber security certification framework, intended as an EU-wide rule for cyber security certifications. Various schemes will specify the purpose and the security standards that should be met and the evaluation methodology.

5G Security in the EU: the 5G Toolbox

Against the backdrop of increasing fears related to the roll-out of foreign 5G technology in EU countries, in January 2020 the Commission released the **5G toolbox** with a view to provide a coordinated EU approach on the secure deployment of 5G.

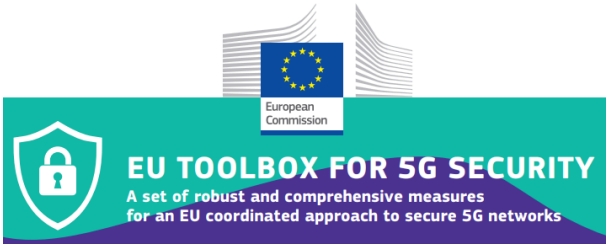
The toolbox is addressed to member states, the Commission and the NIS cooperation group.

Member states should:

- strengthen **security requirements**
- apply **restrictions** to high risk suppliers
- **avoid any major dependency** on one supplier by adopting a multi-vendor strategy – especially, avoid major dependencies with high risk suppliers

The Commission, together with Member States, should:

- maintain a **diverse 5G supply chain** by making use of instruments such as the screening of potential foreign investments concerning 5G assets and further strengthening EU capacities in 5G and post-5G technologies
- develop **relevant EU certification schemes** so to ensure high level of security standardization



Read the [EU factsheet on 5G security] (https://op.europa.eu/en/publication-detail/-/publication/a9d278f6-4637-11ea-b81b-01aa75ed71a1) in detail.
The European Commission, https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security

The NIS Cooperation Group should:

- review periodically the national and **EU risk assessments** on the security of 5G and post 5G networks
- monitor and evaluate the **implementation** of the toolbox
- coordinate and support the implementation of **supporting actions** aimed at the elaboration of guidance and exchange of best practices
- continue convergence of **technical and organizational security requirements** for network operators

Tackling Terrorism Online: EU Approach on Preventing Terrorist Content Online

In 2018, the European Commission submitted a **proposal for the prevention of terrorist content online**. The proposal foresees:

- Terrorist content should be removed in one hour following a **removal order** by national authorities.
- Hosting services should take proactive measures to better **protect their services** and users from terrorist content.
- Service providers and member states should designate **24/7 points of contact** to follow up on removal orders.
- Safeguards to **handle complaints** related to erroneous removals should be created.
- Hosting services and member states will have to **report their actions** in transparency and accountability reports.
- Systematic failures to deal with removals result in **strong penalties**.

> My Commission has prioritised security from day one – we criminalised terrorism and foreign fighters across the EU, we cracked down on the use of firearms and on terrorist financing, we worked with internet companies to get terrorist propaganda offline and we fought radicalisation in Europe's schools and prisons. But there is more to be done."
>
> Jean-Claude Juncker, State of the Union Address, Strasbourg, 2016

European Commission President Jean-Claude Juncker during his State of the Union Address.
European External Action Service (CC BY-NC 2.0)

EU Cyber Diplomacy and Capacity Building

The main goal of EU cyber diplomacy is to preserve a **free, open and secure** cyberspace, considered as the backbone of modern societies.

Free means promoting and protecting human rights and fundamental freedom in cyber space.

Open means a cyber space that is universal, affordable and whose access is equal to everyone.

Secure means having a safe environment in which cyber security measures are strengthened and cooperation is improved against cyber crime. This also means to increase resilience against cyber attacks through diplomatic and legal tools.

EU **cyber diplomacy's main objective** is to make sure the main stakeholders around the world understand the importance of a free, open and secure cyber space. This is done through:

- protecting human rights and fundamental online freedoms
- enhancing competitiveness, growth and prosperity
- promoting sustainable digital development in third countries
- promoting a rule-based cyber space
- shaping rules of internet governance
- engaging with key partners.

In focus: **Cyber security capacity building**

The EU is an active player in building cyber security capacity both within its borders and outside. The main line of actions are of EU external capacity building are:

- supporting national cyber strategies
- increasing capacity of the justice systems
- increasing incident handling
- developing education, professional training and expertise as well as awareness
- applying a whole society approach.

In 2018, the EU published the **Operational Guidance for the EU's International Cooperation on Cyber Capacity Building** and in 2019 funded a large-scale project called Cyber4Dev with a geographical focus on Africa and South Asia.

EU Cyber Measures in Foreign, Security and Defence Policy

In this video lecture, you will learn about:

- the Cyber Diplomacy Toolbox
- the Cyber Defence Policy Framework

The EU Cyber Diplomatic Toolbox and the Cyber Defence Policy Framework are two examples of Brussels' approach in the foreign security and defence aspects of cyber policy.

The **EU Cyber Diplomatic Toolbox** is a joint framework for an EU diplomatic response to malicious cyber activities. The framework was developed by member states and the EEAS and it is part of the European approach to conflict prevention and mitigation in the cyber arena. The Toolbox has the overall goal of **supporting a rule-based cyber space** through the **application of international law** and **promotion of responsible norms** of state behaviour. The framework was established to incorporate the full continuum of EU policies and instruments in case of major external cyber attacks, including, if necessary, restrictive measures.

The basis of this framework is the 2017 council conclusions and related implementing guidelines, the adoption of a horizontal cyber sanctions regime and the guidelines on "Coordinated Attribution at EU level" in 2019.

Importantly, the EU autonomous horizontal cyber sanctions regime establishes a **legal framework** to implement sanctions against cyber attacks (or attempted ones) whose effects constitute an external threat to the Union. Moreover, the framework underlines that attribution is a sovereign political decision of a member state and that not all measures foreseen in a hypothetical EU response require attribution.

The EU has been strengthening and improving the legal and operational foundation of this framework through several cyber exercises at the EU level, generally organized by ENISA.

The **EU Cyber Defence Policy Framework** is another EU framework dedicated to the advancement of EU cyber defence policy. The Framework was unveiled for the first time in 2014 and was later updated in 2018. The EDA and the EEAS are the main institutional actors behind it. The Framework recognizes **cyber space as the fifth domain of operations alongside land, sea, air and space**, whose protection and resilience is a necessary prerequisite for EU missions and operations (civilian and military) to succeed.

The Framework streamlines member states and EU efforts in six policy areas. The primary policy areas are the **development of cyber defence capabilities**, as well as the protection of the EU CSDP communication and information networks. In this regard, EU policy is similar and complementary to NATO cyber policy, as we have already explained in chapter 3. Other areas of action include training and exercises, research and technology, civil-military cooperation and international cooperation. Another revision of the Framework is expected by mid-2022.

EU and NATO Cooperation on Cyber

Key moments

- **February 2016**: Technical Arrangement between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the European Union (CERT-EU) was signed.
- **July 2016**: The European Council and NATO signed the Warsaw Declaration, which foresaw enhanced cooperation between the EU and NATO in 7 concrete areas, including cyber security.
- **2016 and 2017**: A common set of proposals was endorsed by the EU and NATO.
- **July 2018**: A second Joint Declaration was signed in Brussels calling for further and demonstrable progress in the implementation of the set of proposals.
- **June 2019**: A fourth progress report on EU-NATO cooperation was released.

EU-NATO cooperation according to the EU
The European Union, https://www.eeas.europa.eu/eeas/eu-nato-cooperation-factsheets_en

Cooperation on cyber security and defence has been concentrating on:

- exchanges on doctrine development
- participation in cyber exercises; Information exchanges on planned training and threat indicators
- briefings on crisis management
- regular meetings

Highlights of this cooperation include:

- cooperation among NATO Computer Incident Response Capability (NCIRC) and CERT-EU
- NATO staff observed Cyber Europe 2018 and EU staff participated in Cyber Coalition 2018

7. Summary and Further Reading

Summary I

Cybersecurity has become one of the buzzwords of our time, though not every malicious **cyber operation** deserves to be called cyber war. There are many operations below the threshold of war, be it **hacktivism, cybercrime, cyberespionage or cyberterrorism**. Nevertheless, what constitutes a **cyber war** has not yet been definitively defined. However, we have already experienced many cyber **incidents in the real world**, which give us an insight into the dangers created by cyberattacks.

When it comes to the **military application** of "cyber", things are rather different than in the analog realm. Starting with defining what an actual **cyber weapon** is, seasoned concepts like deterrence fail to work in cyberspace as it is very hard, almost impossible, to attribute attacks to a certain actor or country.

Moreover, **classic arms control concepts** such as inspections or verification are difficult to implement – some would even say impossible. Consequently, only "softer" approaches such as **non-binding principles** and **confidence-building measures** have been applied to cyberspace so far. This does not mean, however, that stricter measures could not be implemented with greater effort, though here, the debate is only beginning.

Summary II

Because of the strategic implications of cyber security, militaries worldwide have started to develop **offensive and defensive cybersecurity capabilities**. While it is often hard to distinguish between civilian and military capabilities, there are now taxonomies helping us to gauge countries' "cyber power."

There are several **important actors** in cyber space. On one side, one can find the **UK** and the **US**, which have recently developed new policies and instruments, such as the American **"Persistent Engagement"** doctrine or the British **"Active Cyber Defence"** programme. Both the UK and the US have a prominent role in **NATO**, which has developed its own cyber defence whose operational focus is currently on the protection of the Alliance's networks.

On the other side, there are **China** and **Russia**. The first uses cyber space to prepare for "physical" military operations and enable influence operations; the latter uses ICT means to advance its diplomatic claims and economic interest. Whilst there are several differences in their modus operandi, they both consider **information operations** as a valuable instrument in their security and defence policy toolbox.

In addition to nation-states, other relevant actors in the cyber realm are **cyber terrorists**. While one should exercise caution when assessing their threat, the current general consensus is that terrorist organizations are not as advanced as other actors. This is due to difficulties in gathering the right expertise to mount successful cyberattacks against critical Western infrastructure.

Finally, the **EU** has been another prominent actor in cyberspace since its first cybersecurity strategy in 2013. The EU has produced several important cybersecurity policies, including the **Directive on Security of Network and Information Systems** and the **EU Cyber Security Act**; it has also been active in the fight against terrorism online and to ensure 5G security. In foreign and security policy, the **Cyber Diplomacy Toolbox** constitutes an important step forward in preventing foreign cyber intrusions. Finally, it has attempted to coordinate its cyber defence policy with NATO, with a view to increasing information sharing, cooperation among their CSIRTs and doctrine development.

Additional Resources and Further Reading I

International Organisations

- NATO on "Cyber defence" `[https://www.nato.int/cps/en/natohq/topics_78170.htm]`
- United Nations on "Cyber Risks"
- The UNIDIR Cyber Policy Portal `[https://unidir.org/digitalhub#cyberpolicyportal]`
- European Union Agency for Cyber Security `[https://www.enisa.europa.eu/]`

Think Tanks

- PEASEC `[https://www.peacecenter.org/]` Center for Science and Technology for Peace and Security at Darmstadt University
- Stiftung Neue Verantwortung `[https://www.stiftung-nv.de/en]` (SNV) think tank at the intersection of technology and society – covers various topics on cybersecurity (in English)
- International Institute for Strategic Studies `[https://www.iiss.org/blogs/cyber-report]` weekly report on security related cyber issues

Other Collections or Interesting Sites

- EU Non-Proliferation and Disarmament Consortium `[https://www.nonproliferation.eu//thematics/cybersecurity/]` collection of text on cybersecurity written by members of the EU Non-Proliferation and Disarmament Network
- The Cyber Vault Project `[https://nsarchive.gwu.edu/project/cyber-`

vault-project] online resource documenting cyber activities of the US and foreign governments as well as international organizations – **Highly recommended!**
- Cybersecurity Visuals [https://cltc.berkeley.edu/cybervisuals/] fee images that visualize cybersecurity challenges and how they can be – **Highly recommended!**
- DARKReading [https://www.darkreading.com/] tech-heavy site but well informed about current IT security incidents and latest developments
- Fifth Domain [https://www.c4isrnet.com/cyber/] website covering cyber issues with a strong focus on military aspects

Additional Resources and Further Reading II

General Works

- Brantly, Aaron F./ Van Puyvelde, Damien (2019): Cybersecurity: Politics, Governance and Conflict in Cyberspace, Oxford: Polity Press.
- Reardon, Robert/Choucri, Nazli (2012): The Role of Cyberspace in International Relations: A View of the Literature [https://nchoucri.mit.edu/sites/default/files/documents/%5BReardon,%20Choucri%5D%202012%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf]. In ISA Annual Convention, San Diego.
- Singer, Peter W./Friedman, Allan (2014): Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford: Oxford University Press.
- Whyte, Christopher/Mazanec, Brian (2019): Understanding Cyber Warfare. Politics, Policy and Strategy. London/New York: Routledge.

Deterrence and Arms Control

- Libicki, Martin C. (2009): Cyberdeterrence and Cyberwar [https://books.google.it/books?hl=it&lr=&id=MJX6jL6IeF0C&oi=fnd&pg=PP1&dq=Martin+libicki&ots=HtsjaOwZIi&sig=-wEEAnAM7XMVRxv525OIKaNsI6s#v=onepage&q=Martin%20libicki&f=false]. Rand Corporation.
- Denning, Dorothy E. (2001): Obstacles and Options for Cyber Arms Control [https://www.cyberloop.org/files/cyber-arms-control.pdf]. Arms Control in Cyberspace, Berlin: Heinrich Böll Foundation, p.1–13.
- Reuter, Christian (ed.) (2019): Information Technology for Peace and Security. IT Applications and Infrastructures in Conflicts, Crises, War, and Peace [https://link.springer.com/book/10.1007/978-3-658-25652-4], Wiesbaden: Springer, p. 207–232.
- Valeriano, Brandon/Jensen, Benjamin/Maness, Ryan C. (2018): Cyber Stratey: The Evolving Character of Power and Coercion, Oxford: Oxford University Press.

Various Cyber Issues

- Giacomello, Giampiero (2004): Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism, Studies in Conflict and Terrorism [https://www.tandfonline.com/doi/abs/10.1080/10576100490483660], 27(5): 195—212.
- Giantas, Dominika/Stergiou, Dimitrios (2018): From Terrorism to Cyber-Terrorism: The Case of ISIS [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135927].