



Course material

Course:

**Understanding the digital supply chain and its stakes for humanitarian actors**

Video:

## **4.2 State-sponsored Cyber Operations and Attribution**

Concepts (extracted from automatically generated subtitles):

**State-sponsored cyber operations. State-level cyber operations. Attacker objectives. First gulf war. Cyber operations. Attacker conducts. Establishment of the us cyber command. Introductory video. Strategic importance. Military domain. Recent years. Cyber kill chain. Intelligence agencies. Well-known essay. First information war.**



[to video sequence search](#)

(within Understanding the digital supply chain and its stakes for humanitarian actors.)



[to video](#)

Center for Digital Education. More educational support material here:

<https://www.epfl.ch/education/educational-initiatives/cede/educational-technologies-gallery/boocs-en/>

page 1/37



# CYBERSECURITY

LANDSCAPE OF CYBERTHREATS AND  
GEOPOLITICAL IMPLICATIONS

## State-Sponsored Cyber Operations

Dr. Myriam Dunn Cavelty  
Center for Security Studies, ETH Zürich



...

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....


.....

summary

.....

.....

0m 0s



# You Will Learn



**Cyberspace as a military domain**



**What does it take to conduct cyber-effects-operations?**



**What are cyber-operations mainly used for?**

Hello and welcome. In this introductory video, you are going to learn about state-sponsored cyber operations. You will learn about cyberspace as a military domain, what it takes to conduct state-level cyber operations, and what cyber operations are mainly used for.

notes

summary

0m 4s



# The Militarization of Cyberspace



The military's engagement with cyberspace dates to at least the early 1990s. The First Gulf War was labelled the First Information War due to its significant media and information component.

notes

summary

0m 23s



# The Militarization of Cyberspace



Following this, the US began developing new doctrines and ideas as seen in the well-known essay, Cyberwar is Coming.

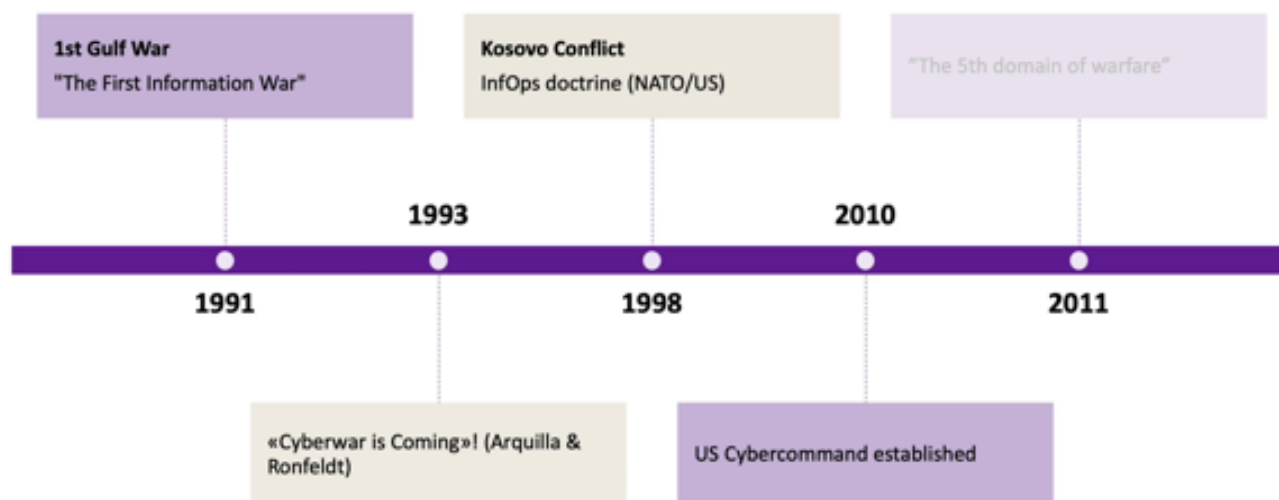
notes

summary

0m 37s



# The Militarization of Cyberspace



In 1998, during the Kosovo Conflict, NATO and the US introduced a new doctrine focusing on the use of information sphere as a crucial element in warfare. By 2010, the establishment of the US Cyber Command marked a pivotal moment as it became one of the first dedicated military units to address cyber threats.

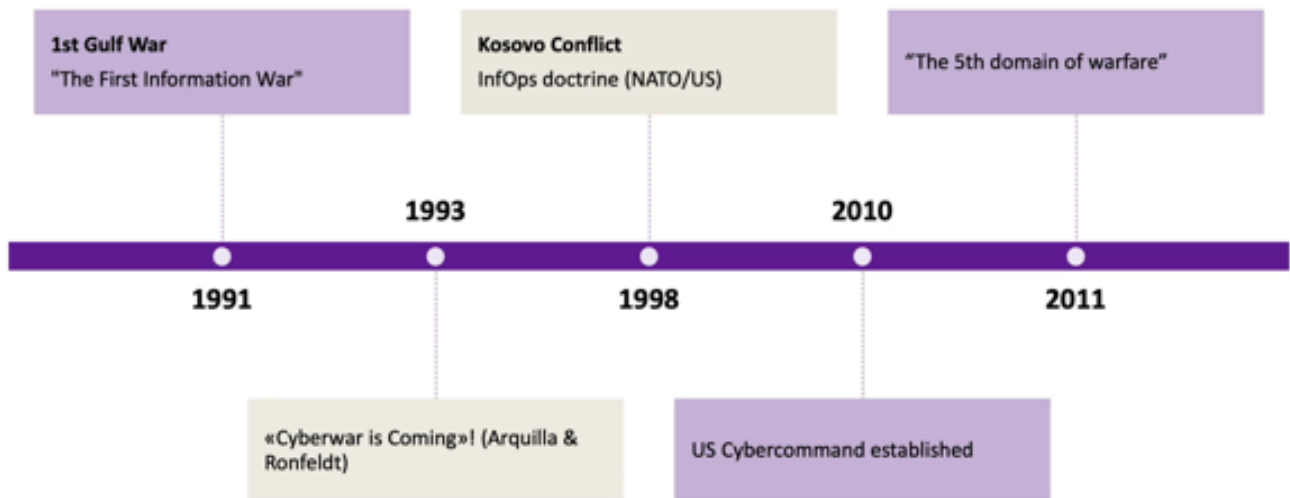
## notes

## summary

0m 49s



# The Militarization of Cyberspace



In 2011, the Pentagon officially declared cyberspace the fifth domain of warfare, alongside land, sea, air, and space.

notes

summary

1m 12s



# Military Cybercommand



Like traditional security dilemmas, when one state develops cyber capabilities, other states may perceive these actions as a threat. This often triggers a cycle of escalation with states expanding their own cyber capabilities in response. This dynamic is evident in the proliferation of military cyber commands worldwide.

## notes

---

---

---

---

---

---

---

---

---

---

## summary

1m 24s



---

---

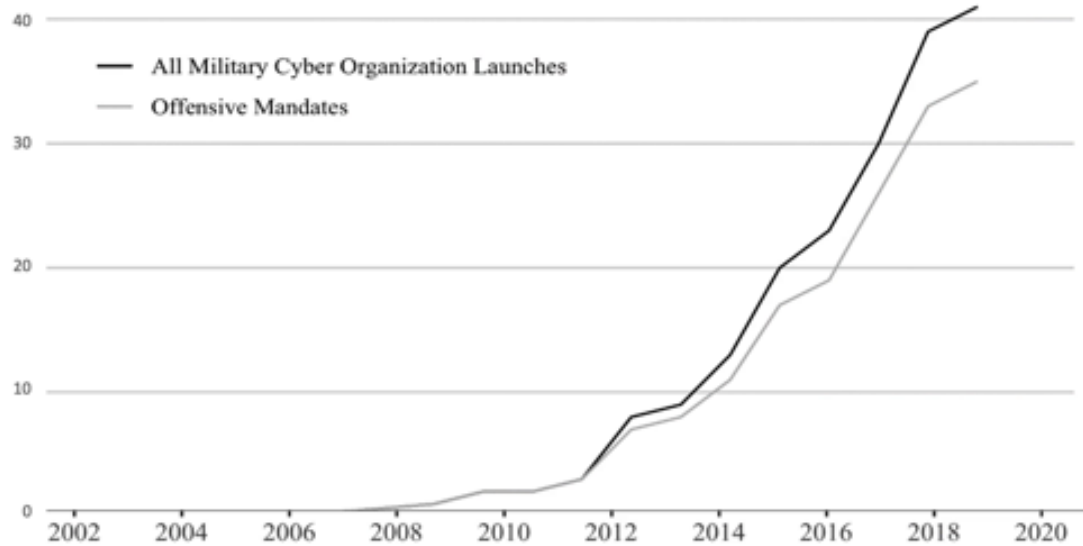
---

---

---



# Military Cybercommand



In recent years,

notes

summary

1m 47s



# Military Cybercommand



there has been a sharp increase in the number of these commands, many of which have offensive mandates, although specific details are closely guarded.

notes

summary

1m 49s



# Military Cybercommand



Currently, there are more than 40 publicly established military cyber commands with over 30 possessing mandates to conduct offensive cyber operations.

## notes

---

---

---

---

---

---

---

---

---

---

## summary

2m 1s



---

---

---

---

---

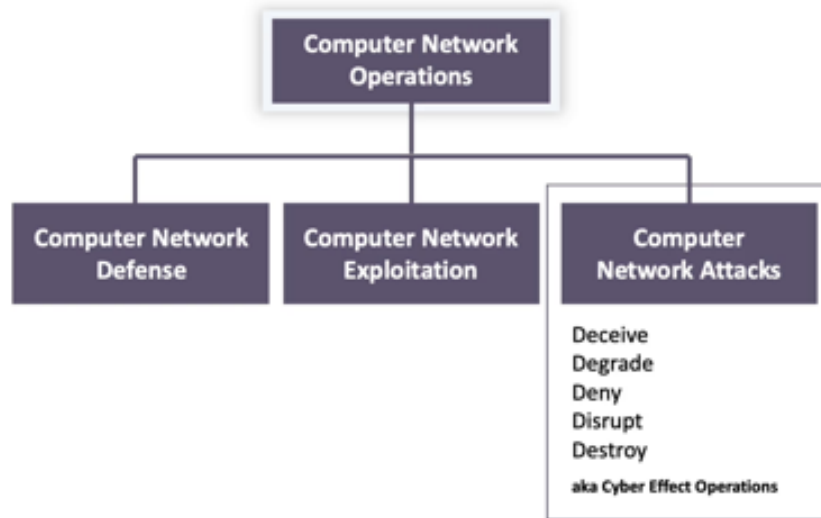
---

---

---

---

---



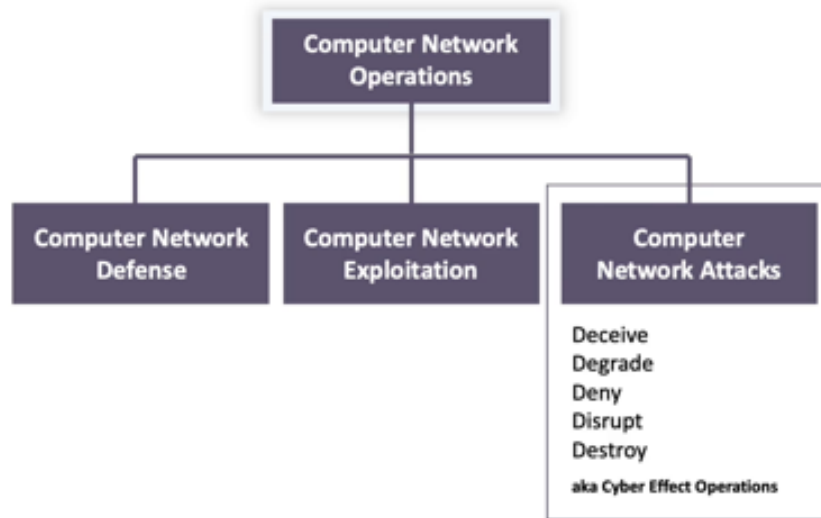
Last, computer network attacks, also known as cyber effect operations,

notes

summary

2m 10s





involve using a combination of technological, human, and organisational resources to achieve specific outcomes. These can include denying, degrading, disrupting, deceiving, or destroying digital data, services, or networks.

notes

summary

2m 18s



# Capabilities Needed



State-sponsored cyber operations are far more sophisticated and resource-intensive than the common stereotype of a few hackers working in isolation. These operations require advanced technical capabilities, a highly skilled workforce, and extensive infrastructure. They are also carefully coordinated with intelligence agencies and military resources, reflecting the strategic importance, government's place on cyber operations as a tool, to achieve national objectives in the digital age.

## notes

---

---

---

---

---

---

---

---

---

---

## summary

2m 36s



---

---

---

---

---

# Capabilities Needed



Personal

Equipment

Training

Intelligence

Organisation

PETIO Framework: Max Smeets, «No Shortcuts» (2022)

In his book No Shortcuts, ETH Zurich-based scholar Max Smeets introduced the PETIO framework which outlines the essential components needed for state-led cyber operations.

notes

summary

3m 9s



# Capabilities Needed



Personal

Equipment

Training

Intelligence

**Organisation**

PETIO Framework: Max Smeets, «No Shortcuts» (2022)

Personnel, equipment, training, intelligence, and organisation.

notes

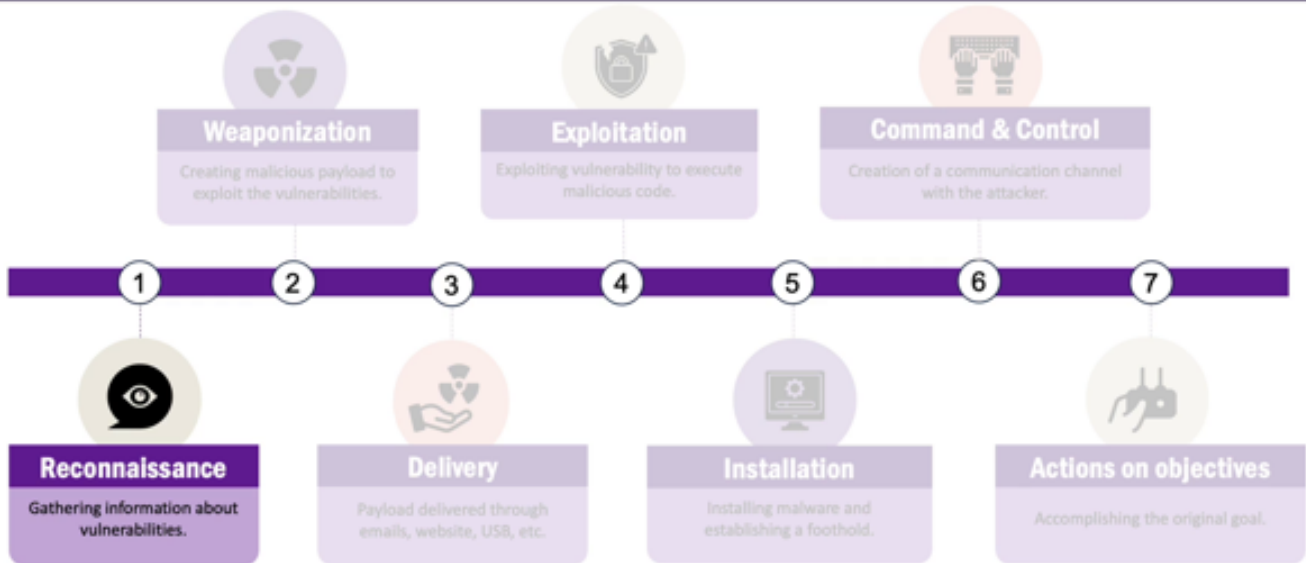
summary

3m 23s





# The Cyber Kill Chain



The cyber kill chain describes seven stages of a cyberattack, from initial reconnaissance to achieving the attacker objectives, highlighting once more that cyber operations take time and patience. Let's go through the steps. Step one, reconnaissance.

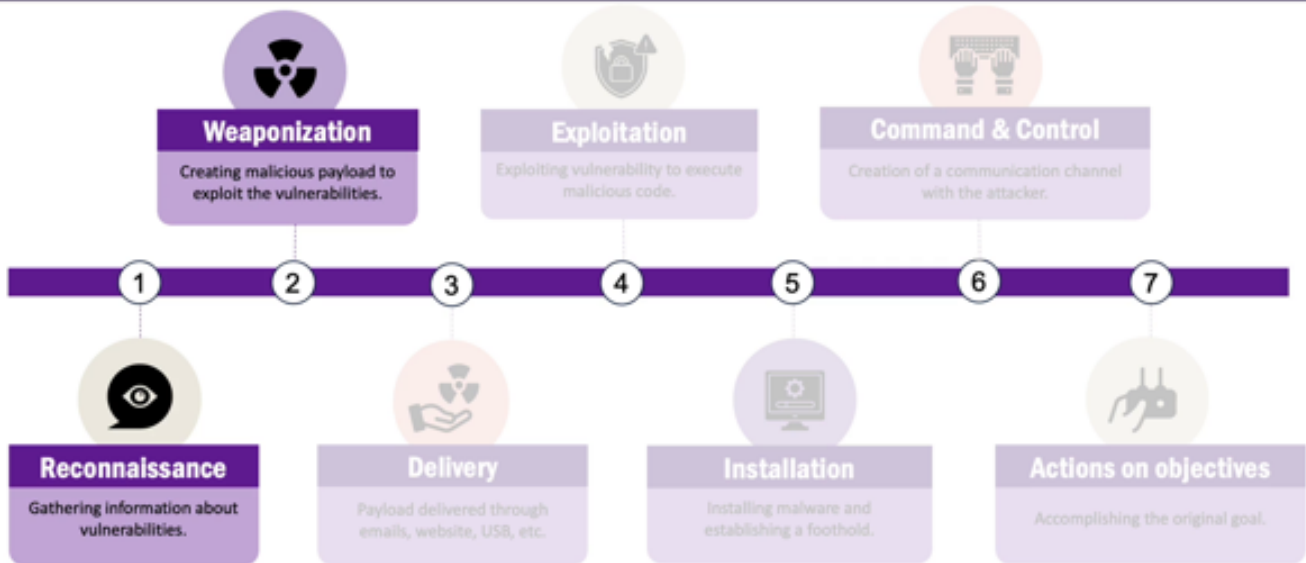
notes

summary

3m 29s



# The Cyber Kill Chain



Here, the attacker conducts research to gather information about the target, such as identifying network structures, personnel, or vulnerabilities. Step two, weaponisation.

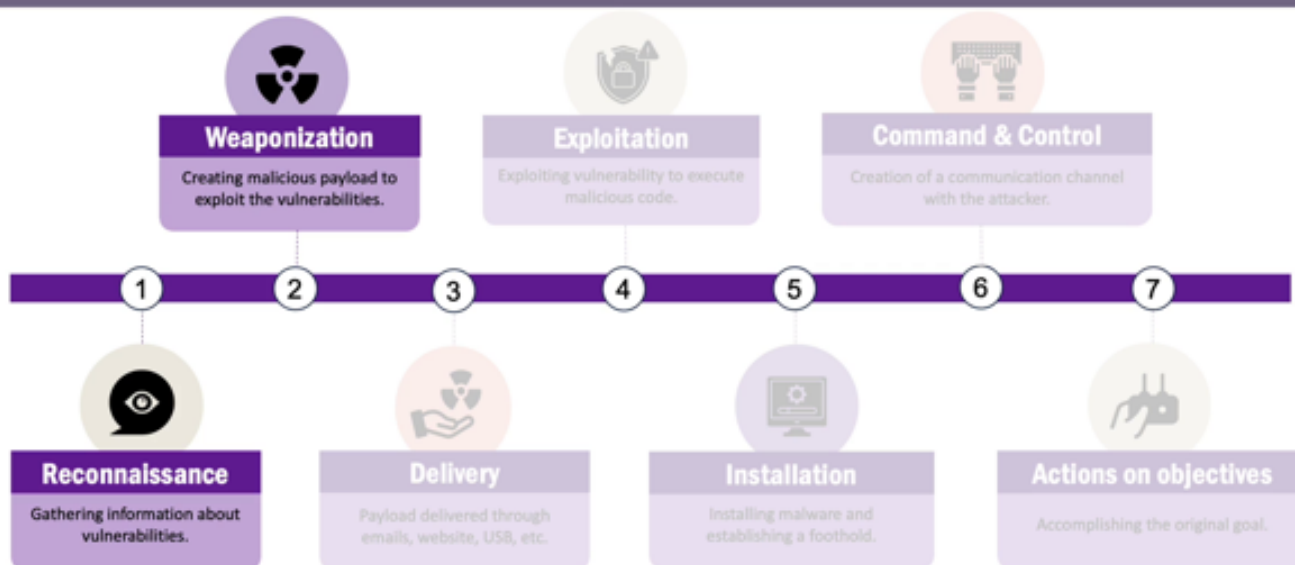
notes

summary

3m 49s



# The Cyber Kill Chain



The attacker creates or modifies a malicious payload,

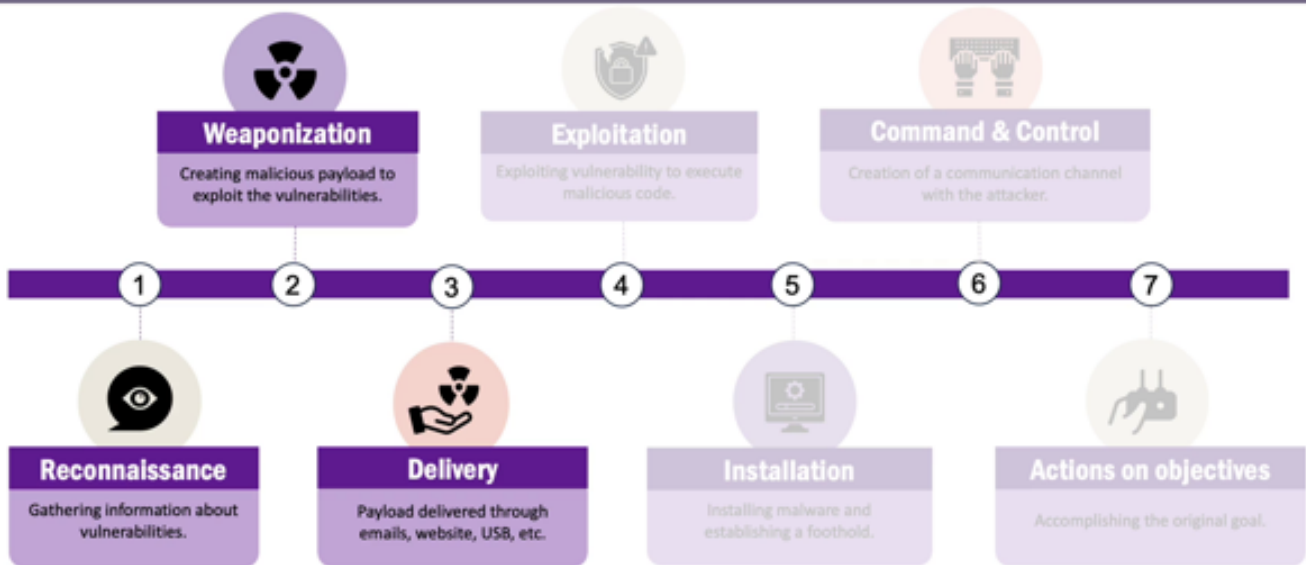
notes

summary

4m 1s



# The Cyber Kill Chain



for example, malware or ransomware, that can exploit the identified vulnerabilities. Step three, delivery. The attacker delivers the payload to the target through, for example,

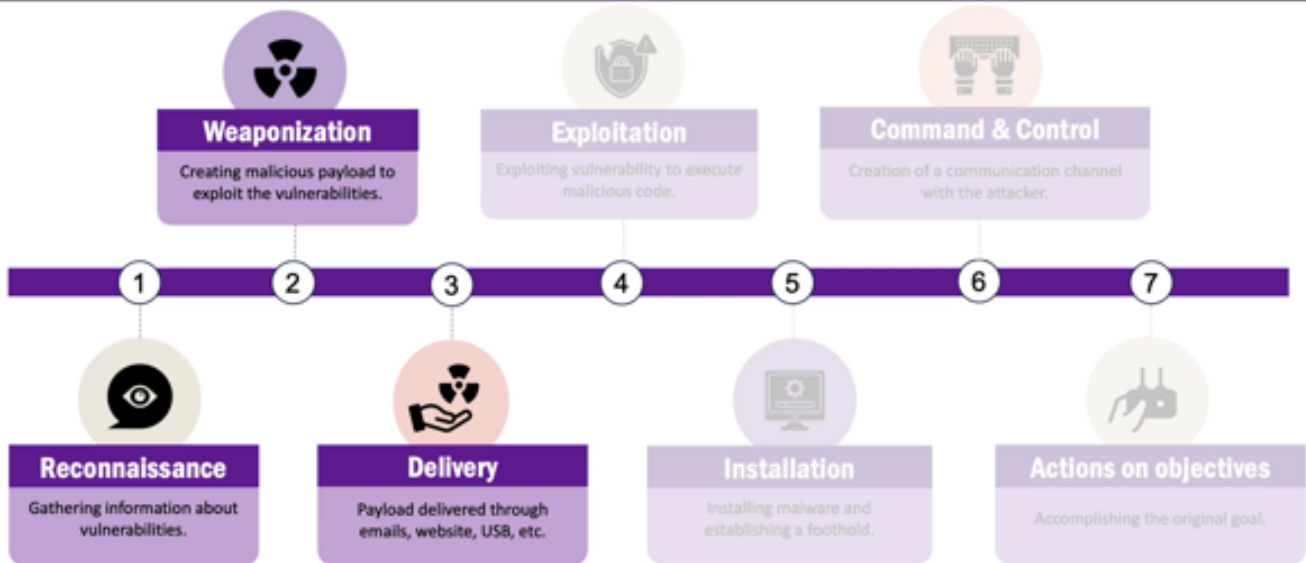
notes

summary

4m 2s



# The Cyber Kill Chain



phishing emails, infected attachments, or compromised web sites or other methods.

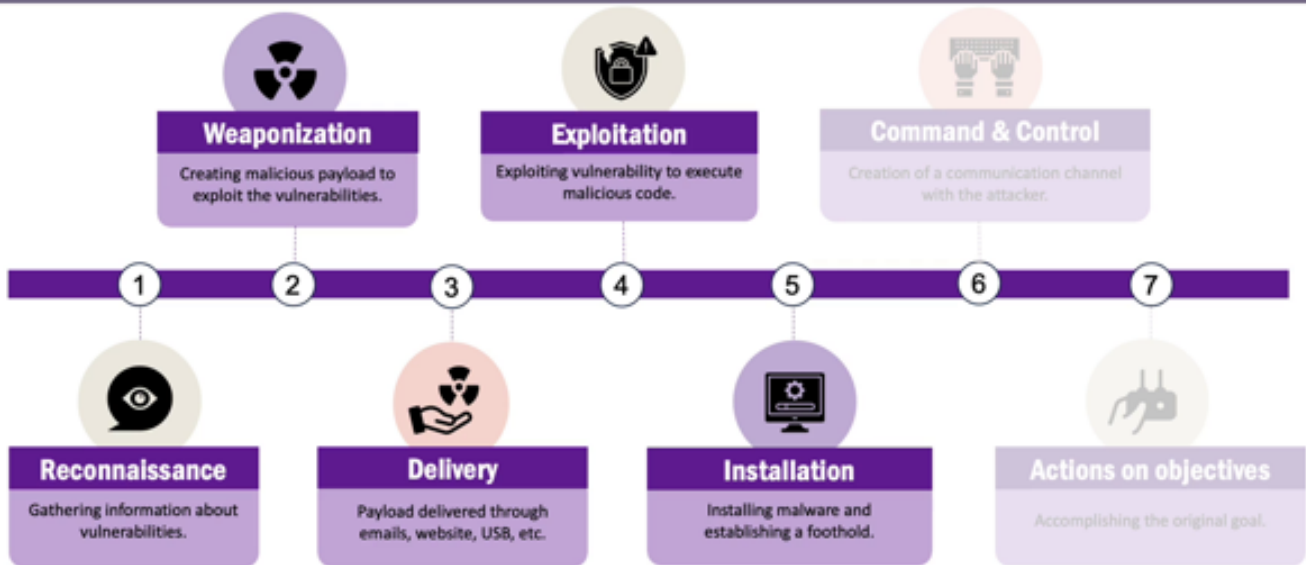
notes

summary

4m 20s



# The Cyber Kill Chain



Step four, exploitation. Once the payload reaches the target, it takes advantage of vulnerabilities such as unpatched software, to execute the malicious code on the target system. Step five, installation. After exploitation, the malware is installed on the target system.

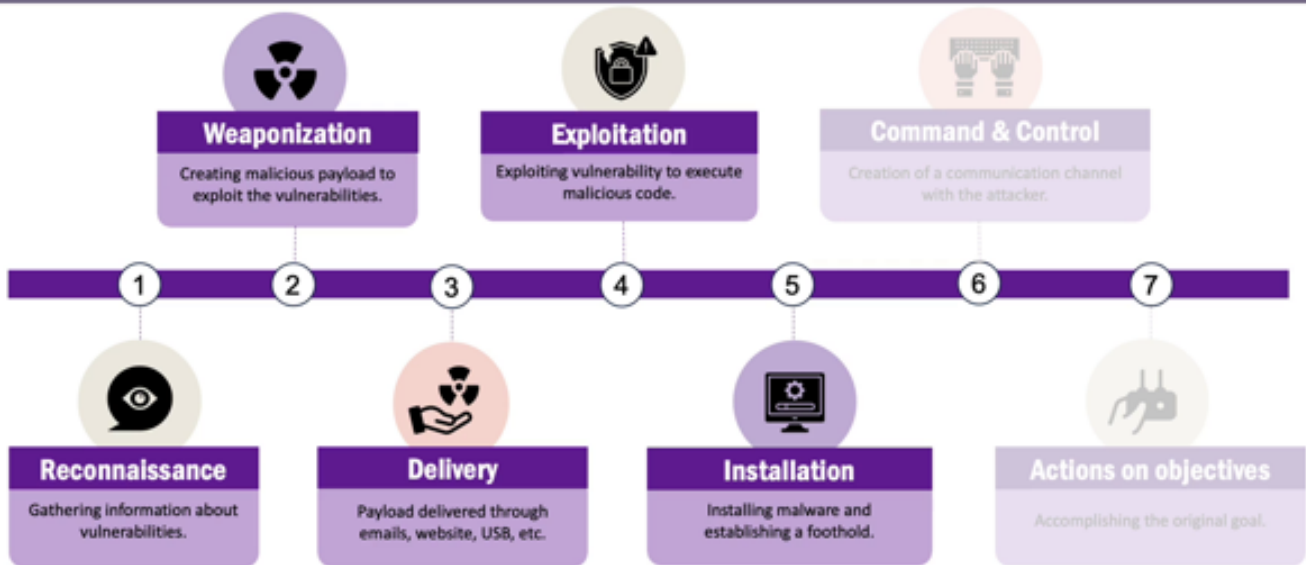
notes

summary

4m 25s



# The Cyber Kill Chain



This step allows the attacker to establish a foothold in the network

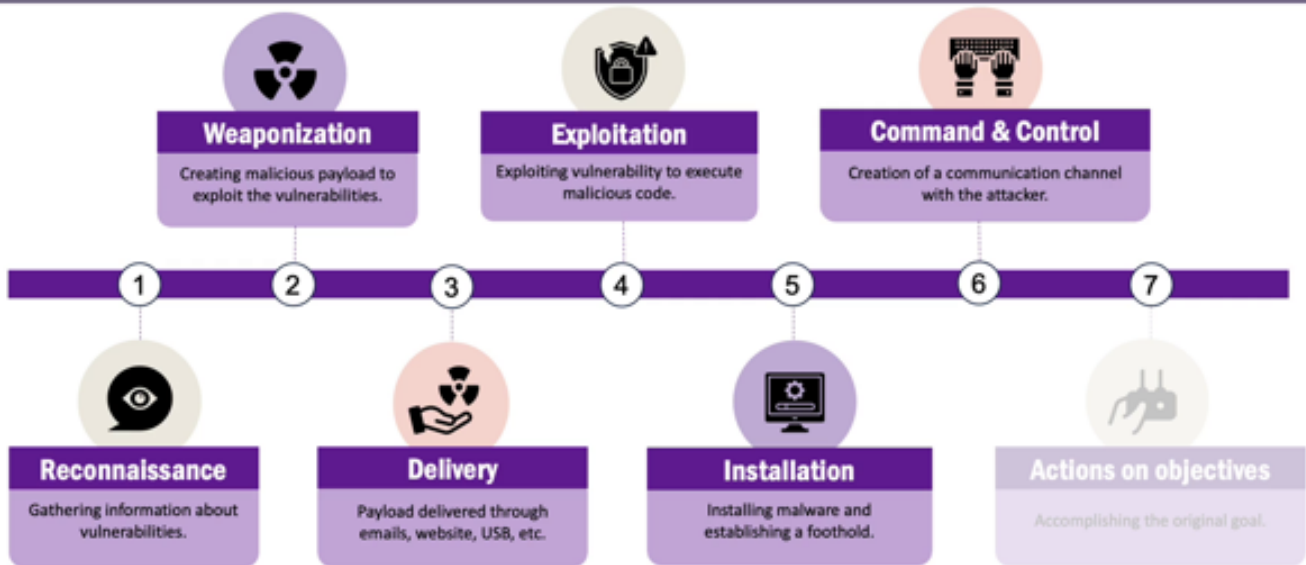
notes

summary

4m 48s



# The Cyber Kill Chain



and maintain persistence. Step six, command and control, or C2. The attacker creates a communication channel

notes

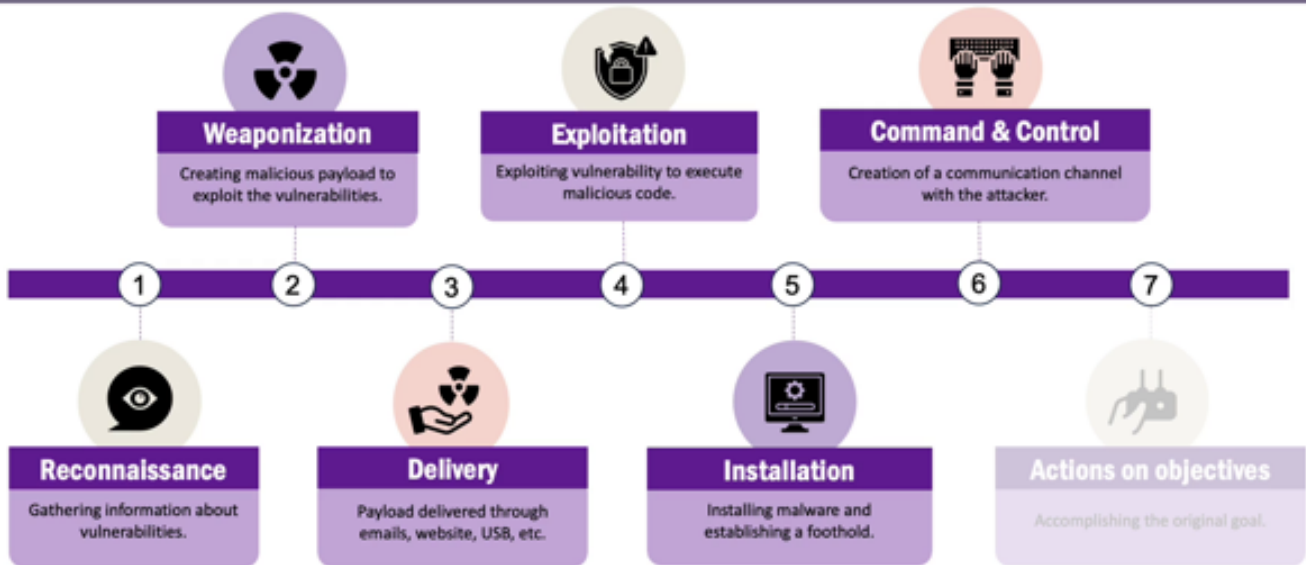
summary

4m 49s





# The Cyber Kill Chain



between the compromised system and their own infrastructure. This allows them to remotely control the infected system

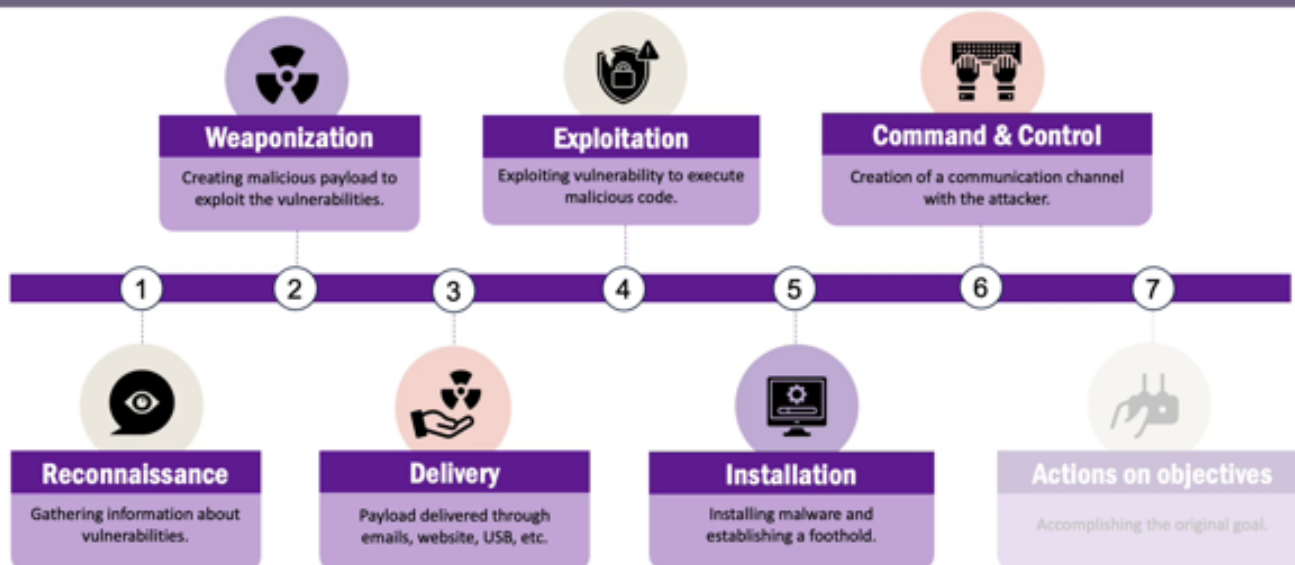
notes

summary

5m 1s



# The Cyber Kill Chain



and send further instructions.

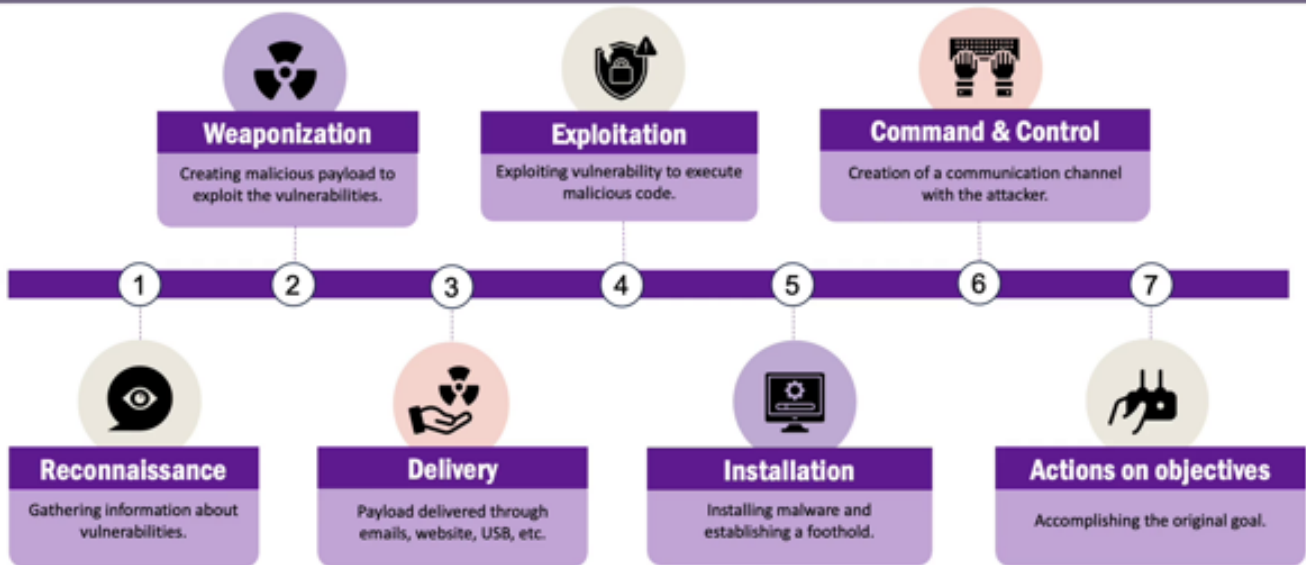
notes

summary

5m 10s



# The Cyber Kill Chain



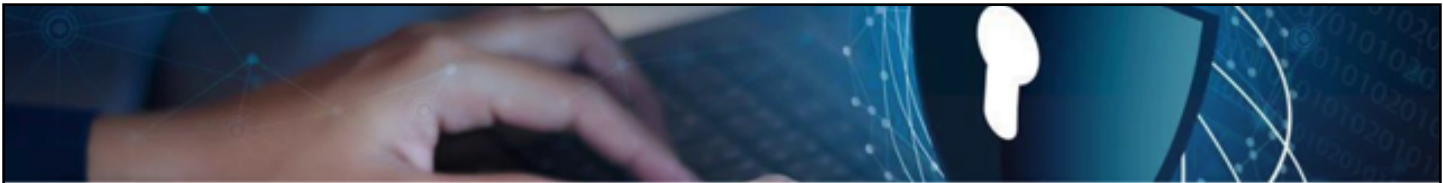
Step seven, actions on objectives. Finally, the attacker achieves their goals, which can include data theft, destruction of data, disruption of services, or moving laterally within the network to compromise other systems.

notes

summary

5m 13s





**Cyber operations are non trivial,  
even more so when considering:**

- International law and order.
- Collateral damages and other undesired consequences.
- Disruption of intelligence operations.



Balancing tactical gains with broader legal,  
diplomatic and strategic consequences.



That means that cyber operations are non-trivial, especially constrained actors

notes

---

---

---

---

---

---

---

---

---

---

summary

5m 31s



---

---

---

---

---

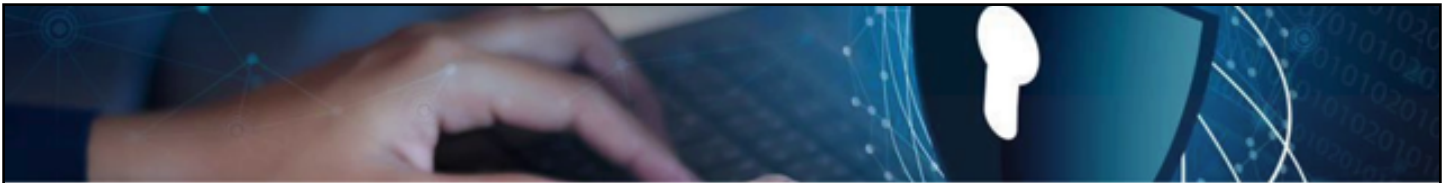
---

---

---

---

---



**Cyber operations are non trivial,  
even more so when considering:**

- International law and order.
- Collateral damages and other undesired consequences.
- Disruption of intelligence operations.



Balancing tactical gains with broader legal,  
diplomatic and strategic consequences.



that are those who care about international law and order, consider important elements such as targeting, or collateral damage, other undesired consequences such as proliferation. They would also test tools to minimise unintended impacts either on civilians or neutral systems, and they would try to avoid disruptions to ongoing intelligence operations. These considerations help balance tactical gains with broader legal, diplomatic, and strategic consequences.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

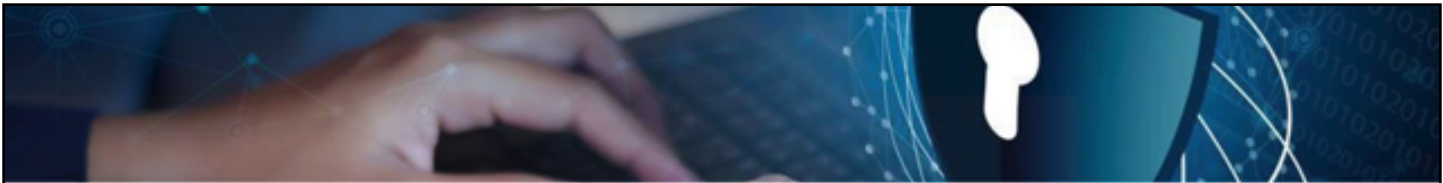
.....

.....

.....

5m 38s





### One simple rule about state-led cyber operations:

- Causing any type of cyber effect at an unspecified point in time is easy.
- Causing targeted cyber effect with a strategic purpose is hard.

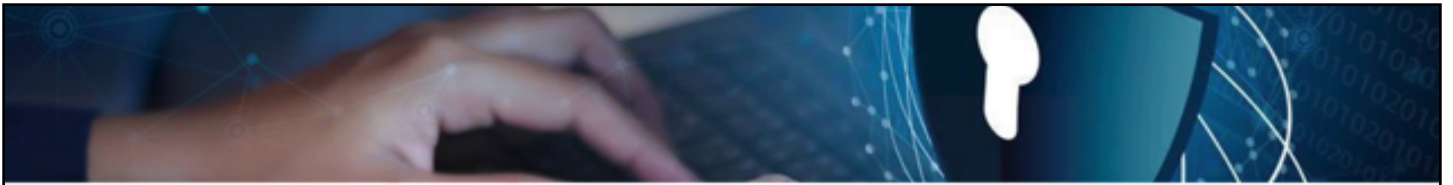
There is one simple rule about state-led cyber operations.

notes

summary

6m 10s





### One simple rule about state-led cyber operations:

- Causing any type of cyber effect at an unspecified point in time is easy.
- Causing targeted cyber effect with a strategic purpose is hard.

On the one hand, causing any type of cyber effect against any system or computer network at an unspecified point in time is easy. Whereas causing a specific targeted cyber effect

### notes

---

---

---

---

---

---

---

---

---

---

### summary

6m 16s



---

---

---

---

---

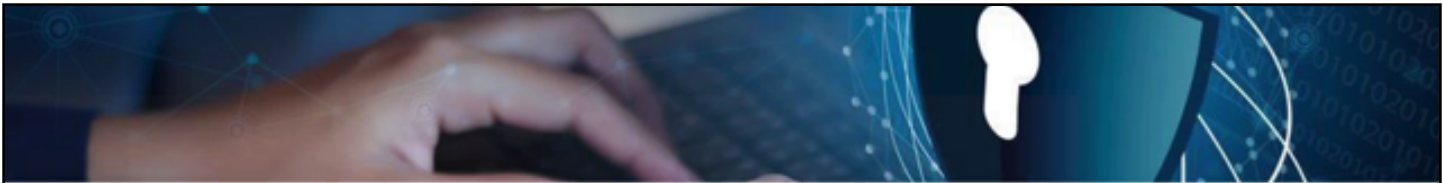
---

---

---

---

---



### One simple rule about state-led cyber operations:

- Causing any type of cyber effect at an unspecified point in time is easy.
- Causing targeted cyber effect with a strategic purpose is hard.

at the designated point in time which achieves a strategic purpose and outweighs the impact of negative consequences is hard.

### notes

---

---

---

---

---

---

---

---

---

---

### summary

6m 32s



---

---

---

---

---

---

---

---

---

---



# What Are They Mainly Used For?



Type of Incident



Data: Council of Foreign Relations "Cyber Operations Tracker" (COT)  
Center for Security Studies at ETH Zürich (dataset available for download) <https://www.cfr.org/cyber-operations/>

Given all this, about 80% of known cyber-operations done by states are stealthy and focused primarily on information extraction or espionage. Cyber espionage has become the predominant form of state-sponsored cyber activity due to its high strategic value, offering critical intelligence at relatively low risk and cost without escalating into open conflict.

## notes

---

---

---

---

---

---

---

---

---

---

## summary

6m 39s



---

---

---

---

---

---

---

---

---

---

# Summary



(Some) states began to build up cyber capabilities in the 2000s.

States use cyber especially for espionage / covert action; few "disruptive actions", hardly any physical destruction (beyond data wiping).

Most state actors operate continuously below the threshold of armed conflict to gain strategic advantage or weaken institutions → realm of intelligence operations.

In sum, states began building their cyber capabilities in the 2000s with a significant acceleration around 2014.

notes

summary

7m 9s



# Summary



(Some) states began to build up cyber capabilities in the 2000s.

States use cyber especially for espionage / covert action; few "disruptive actions", hardly any physical destruction (beyond data wiping).

Most state actors operate continuously below the threshold of armed conflict to gain strategic advantage or weaken institutions → realm of intelligence operations.

These capabilities are primarily used for espionage and covert action, while disruptive actions are rare, and physical destruction is minimal, mostly limited to data wiping.

## notes

---

---

---

---

---

---

---

---

---

---

## summary

7m 18s



---

---

---

---

---

---

---

---

---

---

# Summary



(Some) states began to build up cyber capabilities in the 2000s.

States use cyber especially for espionage / covert action; few "disruptive actions", hardly any physical destruction (beyond data wiping).

Most state actors operate continuously below the threshold of armed conflict to gain strategic advantage or weaken institutions → realm of intelligence operations.

Most state actors operate below the threshold of armed conflict, aiming to gain strategic advantages or weaken institutions, activities that fall square within the realm of intelligence operations.

notes

summary

7m 30s



## Image reference



### In order of appearance

PICTURE 1: By Kizito from Adobe Stock  
PICTURE 2: By Jitapon from Adobe Stock  
ICON1: Created by Ade Nur Hidayat from Noun Project  
ICON2: Created by Ahman Muggalla from Noun Project  
ICON3: Created by Nihinan Telah from Noun Project  
PICTURE 3: By Justlight from Adobe Stock  
PICTURE 4: By saravut sy from Adobe Stock  
PICTURE 6: By Kakaba sy from Adobe Stock

This brings unique challenges for international relations and international law, particularly around attribution, sovereignty, and the norms governing state behaviour in cyberspace.

#### notes

---

---

---

---

---

---

---

---

---

---

#### summary

7m 44s



---

---

---

---

---