

Course material

Course:

Understanding the digital supply chain and its stakes for humanitarian actors

Video:

4.1 The Cyberthreat Landscape

Concepts (extracted from automatically generated subtitles):

Landscape of cyber threats. Criminal landscape. Threat actors. State actors. Annual cost of cybercrime. Similar picture. Steady increase. Integration of physical devices. Criminal groups. Quality of recent cyber threats. Introductory video. Top organised crime groups. Myriam dunn cavelty. Cyber operations. Different kinds of cyber threats.



[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/>

CYBERSECURITY PART I

GEOPOLITICS AND LEGAL CONSIDERATIONS



.....



.....



.....



...

notes

summary

0m 0s



CYBERSECURITY

LANDSCAPE OF CYBERTHREATS AND GEOPOLITICAL IMPLICATIONS



The Cyberthreat Landscape

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



Hello and welcome.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....


.....

summary

.....

.....

0m 9s



The Cyberthreat Landscape



I am Myriam Dunn Cavelty, Senior Scientist at the Centre for Security Studies at ETH Zurich. In this introductory video, you are going to learn about the landscape of cyber threats.

notes

summary

0m 13s



You Will Learn



Threat Exposure:

Understanding quantity and quality of recent cyber-threats.



Type of Threat Actors:

Identify who they are and their motivations.



Types of Cyberthreats:

Explore various forms of cyber threats.

You will learn about threat exposure, mainly about the quantity and quality of recent cyber threats. You will learn about threat actors, who they are, and why they are doing what they are doing. And you will hear about different kinds of cyber threats.

notes

summary

0m 29s



You Will Learn

Let us start by looking at the graphic

notes

summary

0m 48s





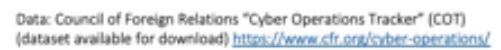
that estimates the annual cost of cybercrime worldwide. Though just an estimation, and to be taken as such, you can clearly see a steady increase over the years. Other estimations by different analysts all show the same tendency, a clear upwards trend.

notes

summary

0m 49s





notes

summary

1m 13s



Threats - Quantity and Quality



MORE

- Ca. 95% are criminal in nature
- Better analytical capabilities = we see more!

BIGGER

- In 2023, the average cost of a data breach was 4.45M USD
- In 2023, 1.1B USD received by ransomware actors (+140% from 2022)

BETTER

- More cyber-attacks are targeted
- More cyber-attacks are sophisticated

The quantity and the quality of cyber threats has increased over the years. Two things are important to note about the increase in quantity.

notes

summary

1m 33s



Threats - Quantity and Quality



MORE

- Ca. 95% are criminal in nature
- Better analytical capabilities = we see more!

BIGGER

- In 2023, the average cost of a data breach was 4.45M USD
- In 2023, 1.1B USD received by ransomware actors (+140% from 2022)

BETTER

- More cyber-attacks are targeted
- More cyber-attacks are sophisticated

First, around 95% of all of them are criminal in nature, which means they are conducted by non-state actors, and only a very small percentage is attributable to state actors. Second, the increase in quantity is also correlated to much better analytical capabilities on the side of the defenders. We simply see much more than we used to.

notes

summary

1m 44s



Threats - Quantity and Quality



MORE

- Ca. 95% are criminal in nature
- Better analytical capabilities = we see more!

BIGGER

- In 2023, the average cost of a data breach was 4.45M USD
- In 2023, 1.1B USD received by ransomware actors (+140% from 2022)

BETTER

- More cyber-attacks are targeted
- More cyber-attacks are sophisticated

But cyber threats do not only increase in quantity, they also become bigger. In 2023, the global average cost of a data breach was \$4.45 million, which is a 2.25% increase from the previous year. Much more staggering, the total amount of money that ransomware actors received was \$1.1 billion in 2023, and that is an increase of 140% from the previous year.

notes

summary

2m 13s



Threats - Quantity and Quality



MORE

- Ca. 95% are criminal in nature
- Better analytical capabilities = we see more!

BIGGER

- In 2023, the average cost of a data breach was 4.45M USD
- In 2023, 1.1B USD received by ransomware actors (+140% from 2022)

BETTER

- More cyber-attacks are targeted
- More cyber-attacks are sophisticated

The third component is that actors in general get better.

notes

summary

2m 48s



Threats - Quantity and Quality



MORE

- Ca. 95% are criminal in nature
- Better analytical capabilities = we see more!

BIGGER

- In 2023, the average cost of a data breach was 4.45M USD
- In 2023, 1.1B USD received by ransomware actors (+140% from 2022)

BETTER

- More cyber-attacks are targeted
- More cyber-attacks are sophisticated

More cyberattacks than before are targeted, and more cyberattacks are sophisticated, using find particular skills and knowledge about the systems that they target.

notes

summary

2m 49s





Why is it Getting Worse?

Attack surface is growing – Overall security not

- Internet of Things / Cyber-physical systems.
- Digitalization in general.

Professionalization/Specialization

- Cyber Crime-as-a-Service.
- Organized Crime very active and innovative.

State actors and cyberspace

- Increased capabilities for strategic and political goals.
- More time and resources than criminal groups.
- Intelligence ops rather than direct military engagement.

This begs the question, why is it getting worse? First, the attack surface is growing. With rapid digitalisation, the number of potential entry points for cyberattacks

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

3m 6s







Why is it Getting Worse?

Attack surface is growing – Overall security not

- Internet of Things / Cyber-physical systems.
- Digitalization in general.

Professionalization/Specialization

- Cyber Crime-as-a-Service.
- Organized Crime very active and innovative.

State actors and cyberspace

- Increased capabilities for strategic and political goals.
- More time and resources than criminal groups.
- Intelligence ops rather than direct military engagement.

Second, cybercrime is professionalising. The rise of cybercrime as a service has led to a more organised and specialised criminal landscape. Criminals can now easily access tools and services

notes

summary

3m 34s





Why is it Getting Worse?

Attack surface is growing – Overall security not

- Internet of Things / Cyber-physical systems.
- Digitalization in general.

Professionalization/Specialization

- Cyber Crime-as-a-Service.
- Organized Crime very active and innovative.

State actors and cyberspace

- Increased capabilities for strategic and political goals.
- More time and resources than criminal groups.
- Intelligence ops rather than direct military engagement.

tailored for specific types of attacks, making it easier and more efficient for them to carry out cybercrime. Third, state actors also exploit cyberspace.

notes

summary

3m 49s





Why is it Getting Worse?

Attack surface is growing – Overall security not

- Internet of Things / Cyber-physical systems.
- Digitalization in general.

Professionalization/Specialization

- Cyber Crime-as-a-Service.
- Organized Crime very active and innovative.

State actors and cyberspace

- Increased capabilities for strategic and political goals.
- More time and resources than criminal groups.
- Intelligence ops rather than direct military engagement.

They have significantly invested in cyber capabilities, particularly for strategic and political purposes.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

4m 1s





Why is it Getting Worse?

Attack surface is growing – Overall security not

- Internet of Things / Cyber-physical systems.
- Digitalization in general.

Professionalization/Specialization

- Cyber Crime-as-a-Service.
- Organized Crime very active and innovative.

State actors and cyberspace

- Increased capabilities for strategic and political goals.
- More time and resources than criminal groups.
- Intelligence ops rather than direct military engagement.

Unlike criminal groups, these actors have the resources and the time

notes

summary

4m 12s





Why is it Getting Worse?

Attack surface is growing – Overall security not

- Internet of Things / Cyber-physical systems.
- Digitalization in general.

Professionalization/Specialization

- Cyber Crime-as-a-Service.
- Organized Crime very active and innovative.

State actors and cyberspace

- Increased capabilities for strategic and political goals.
- More time and resources than criminal groups.
- Intelligence ops rather than direct military engagement.

to develop and launch sophisticated cyber operations. Instead of outright military engagement, they often conduct covert operations.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

4m 14s



Threat pyramid



Top Tier

APT = advanced persistent threats: well funded, experienced and strategic.

Middle Tier

Better organized, more skills, more dangerous attacks.

Bottom Tier

Largest group, mostly nuisance-level attacks.

One way of looking at the landscape of threat actors is by ways of a so-called threat pyramid. In short, not everyone can do everything. In fact, most threat actors cannot pull off sophisticated targeted attacks. They are at the bottom. Though by far the biggest group, many of their attacks amount to not more than a nuisance.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

4m 25s



.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Threat pyramid



Top Tier

APT = advanced persistent threats: well funded, experienced and strategic.

Middle Tier

Better organized, more skills, more dangerous attacks.

Bottom Tier

Largest group, mostly nuisance-level attacks.

As we move up, we reach the realm of better organised threats.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

4m 48s



.....

.....

.....

.....

.....

Threat pyramid



Top Tier

APT = advanced persistent threats: well funded, experienced and strategic.

Middle Tier

Better organized, more skills, more dangerous attacks.

Bottom Tier

Largest group, mostly nuisance-level attacks.

These actors have better skills, and their actions are potentially more dangerous and damaging.

notes

summary

4m 49s



Threat pyramid



Top Tier

APT = advanced persistent threats: well funded, experienced and strategic.

Middle Tier

Better organized, more skills, more dangerous attacks.

Bottom Tier

Largest group, mostly nuisance-level attacks.

At the very top, we have what is called Advanced Persistent Threats or APTs.

notes

summary

5m 1s



Threat pyramid



Top Tier

APT = advanced persistent threats: well funded, experienced and strategic.

Middle Tier

Better organized, more skills, more dangerous attacks.

Bottom Tier

Largest group, mostly nuisance-level attacks.

They are a small group of threat actors with the biggest skills. They are well-funded, experienced, and strategically thinking. Very often, they are state-affiliated or the top organised crime groups.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

5m 3s



.....

.....

.....

.....

.....

Actor Types per Motivation



Type	Motivation	Capabilities
State Actors / Advanced Persistent Threats (APTs)	espionage, disruption of critical infrastructure, supply chain attacks, influence	High to very high
Criminals – organized, targeted	financial gain, selling information (industrial espionage), intellectual property interests.	Medium to high
Criminals – opportunistic	financial gain	Medium
Hacktivists	political or social statements, discussions, information disclosure, reputational damage.	Low to medium
Individuals	financial gain	Low

Apart from the difference in skill level and available capabilities, these threat actors can also be differentiated by their motivation. Let us look at the different types of threats that derive from this, starting from the bottom.

notes

summary

5m 25s





notes

5m 40s



Actor Types per Motivation



Type	Motivation	Capabilities
State Actors / Advanced Persistent Threats (APTs)	Information gathering, disruption of critical infrastructure, supply chain attacks, influence operations.	High to very high
Criminals – organized, targeted	Blackmail, obtaining and selling information (industrial espionage), mainly financial interests.	Medium to high
Criminals – opportunistic	Financial interests.	Medium
Hacktivists	Disseminating opinions and initiating discussions, gaining attention and/or causing reputational damage.	Low to medium
Individuals	Mischief, curiosity, social pressure,...	Low

to carry out large-scale damaging cyberattacks and often lack the desire to do so, too. Hactivism originally signified a form of political protest

notes

summary

5m 49s



Actor Types per Motivation



Type	Motivation	Capabilities
State Actors / Advanced Persistent Threats (APTs)	Information gathering, disruption of critical infrastructure, supply chain attacks, influence operations.	High to very high
Criminals – organized, targeted	Blackmail, obtaining and selling information (industrial espionage), mainly financial interests.	Medium to high
Criminals – opportunistic	Financial interests.	Medium
Hacktivists	Disseminating opinions and initiating discussions, gaining attention and/or causing reputational damage.	Low to medium
Individuals	Mischief, curiosity, social pressure,...	Low

using online means, but in recent years, hacktivism has also become a method for influence operations. For example, when someone hacks into a system and steal sensitive data that is subsequently leaked to influence a political process.

notes

summary

6m 1s



Actor Types per Motivation



Type	Motivation	Capabilities
State Actors / Advanced Persistent Threats (APTs)	Information gathering, disruption of critical infrastructure, supply chain attacks, influence operations.	High to very high
Criminals – organized, targeted	Blackmail, obtaining and selling information (industrial espionage), mainly financial interests.	Medium to high
Criminals – opportunistic	Financial interests.	Medium
Hacktivists	Disseminating opinions and initiating discussions, gaining attention and/or causing reputational damage.	Low to medium
Individuals	Mischief, curiosity, social pressure,...	Low

Cybercrime, as the most prevalent threat form, is very frequent.

notes

summary

6m 21s





Type	Motivation	Capabilities
State Actors / Advanced Persistent Threats (APTs)	Information gathering, disruption of critical infrastructure, supply chain attacks, influence operations.	High to very high
Criminals – organized, targeted	Blackmail, obtaining and selling information (industrial espionage), mainly financial interests.	Medium to high
Criminals – opportunistic	Financial interests.	Medium
Hacktivists	Disseminating opinions and initiating discussions, gaining attention and/or causing reputational damage.	Low to medium
Individuals	Mischief, curiosity, social pressure,...	Low

notes

summary

6m 25s



Actor Types per Motivation



Type	Motivation	Capabilities
State Actors / Advanced Persistent Threats (APTs)	Information gathering, disruption of critical infrastructure, supply chain attacks, influence operations.	High to very high
Criminals – organized, targeted	Blackmail, obtaining and selling information (industrial espionage), mainly financial interests.	Medium to high
Criminals – opportunistic	Financial interests.	Medium
Hacktivists	Disseminating opinions and initiating discussions, gaining attention and/or causing reputational damage.	Low to medium
Individuals	Mischief, curiosity, social pressure,...	Low

State actors are generally the most capable.

notes

summary

6m 46s



Actor Types per Motivation



Type	Motivation	Capabilities
State Actors / Advanced Persistent Threats (APTs)	Information gathering, disruption of critical infrastructure, supply chain attacks, influence operations.	High to very high
Criminals – organized, targeted	Blackmail, obtaining and selling information (industrial espionage), mainly financial interests.	Medium to high
Criminals – opportunistic	Financial interests.	Medium
Hacktivists	Disseminating opinions and initiating discussions, gaining attention and/or causing reputational damage.	Low to medium
Individuals	Mischief, curiosity, social pressure,...	Low

They move in cyberspace with political purpose. They may conduct cyber influence operations, leveraging existing vulnerabilities of the information environment or society more generally

notes

summary

6m 49s



Actor Types per Motivation



Type	Motivation	Capabilities
State Actors / Advanced Persistent Threats (APTs)	Information gathering, disruption of critical infrastructure, supply chain attacks, influence operations.	High to very high
Criminals – organized, targeted	Blackmail, obtaining and selling information (industrial espionage), mainly financial interests.	Medium to high
Criminals – opportunistic	Financial interests.	Medium
Hacktivists	Disseminating opinions and initiating discussions, gaining attention and/or causing reputational damage.	Low to medium
Individuals	Mischief, curiosity, social pressure,...	Low

and rely on tools and techniques to affect audiences.

notes

summary

7m 1s



Actor Types per Motivation



Type	Motivation	Capabilities
State Actors / Advanced Persistent Threats (APTs)	Information gathering, disruption of critical infrastructure, supply chain attacks, influence operations.	High to very high
Criminals – organized, targeted	Blackmail, obtaining and selling information (industrial espionage), mainly financial interests.	Medium to high
Criminals – opportunistic	Financial interests.	Medium
Hacktivists	Disseminating opinions and initiating discussions, gaining attention and/or causing reputational damage.	Low to medium
Individuals	Mischief, curiosity, social pressure,...	Low

Or they use cyber operations to steal classified or sensitive data

notes

summary

7m 6s



Actor Types per Motivation



Type	Motivation	Capabilities
State Actors / Advanced Persistent Threats (APTs)	Information gathering, disruption of critical infrastructure, supply chain attacks, influence operations.	High to very high
Criminals – organized, targeted	Blackmail, obtaining and selling information (industrial espionage), mainly financial interests.	Medium to high
Criminals – opportunistic	Financial interests.	Medium
Hacktivists	Disseminating opinions and initiating discussions, gaining attention and/or causing reputational damage.	Low to medium
Individuals	Mischief, curiosity, social pressure,...	Low

to gain a strategic advantage. Cyber operations that disrupt critical infrastructure or even damage them are rare. Predominantly, cyber operations are activities below the threshold of war.

notes

summary

7m 14s





In order of appearance

PICTURE 1: By robin-worrall Unsplash
PICTURE 2: By Kras99 from Adobe Stock
PICTURE 3: By Touseef from Adobe Stock
ICON1: Created by Balm Icon from Noun Project
ICON2: Created by Ahman Musyaffa from Noun Project
ICON3: Created by Nithinan Tatah from Noun Project
PICTURE 4: By terovesalainen from Adobe Stock
PICTURE 5: By saravut sy from Adobe Stock
PICTURE 6: By Tierney sy from Adobe Stock

In sum, there is a broad range of cyber threats conducted by a broad range of actors whose motivation and skill levels, also called capabilities, differ substantially. The majority of cyberattacks are crime, around about 95%. Cyberattacks are predominantly conducted under the threshold of war.

notes

summary

7m 29s

