Codebook *European Repository of Cyber Incidents* (EuRepoC) 1.0

March 2023

General remarks:
This is a general codebook for the EuRepoC database, explaining all core categories in detail. The numeration does not match the order of the categories within the files "EuRepoC_Global_Database_1.0" and "EuRepoC_EU_Database_1.0" that can be downloaded here.

Codes and sub-codes are separated by ";".

In case of missing values/information, "not available" (na) is coded.

The repository only includes cyber incidents/operations that affected the so-called "CIA-Triad of Information Security", meaning the Confidentiality, Integrity or Availability of the targeted systems. Reported "attempts" or "foiled/thwarted cyber operations" are only included if the targeted networks have been at least infiltrated at some time, meaning that the Confidentiality of the systems has been affected.

1. Incident ID

Uniquely assigned identification number for each Incident.

2. Inclusion criteria / *multiple codings possible*

Code	Subcode	Description
1		Attack conducted by nation state *(generic "state-attribution" or direct attribution towards specific state-entities, e.g., intelligence agencies)*
2		Attack conducted by non-state group / non-state actor with political goals (religious, ethnic, etc. groups) / undefined actor with political goals
	1	Attack conducted by a state-affiliated group (includes state-sanctioned, state-supported, state-controlled but officially non-state actors) ("cyber-proxies") / a group that is *generally* attributed as state-affiliated
3		Attack on (inter alia) political target(s), politicized
4		Attack on (inter alia) political target(s), not politicized
5		Attack on non-political target(s), politicized
6		Attack on critical infrastructure target(s) **NEW**

Remark:
"Political targets" are receiver categories 1 and 2 (see below).

3. Source incident detection / disclosure / *multiple codings possible*

Describes the actor that was the first to disclose the incident.

For example - multiple codings: if a victim reports to a media outlet that it was the target of a cyber operation but DOES NOT publish this information itself, e.g. on its website, AND the media outlet reports about this fact in its article, this category would be coded as 0 AND 1.
BUT: if an unknown victim hires an IT-company to do forensics on its systems after a cyber operation, allows the IT-company to report about the incident but remains unknown in the report, the only code would be 2.

Code	Description
0	Incident disclosed by media *(without further information on source)*
1	Incident disclosed by victim
2	Incident disclosed by IT-security company
3	Incident disclosed by attacker
4	Incident disclosed by any other third-party-actor *(e.g., Citizen Lab, Amnesty International, whistleblowers) or authorities of another state*
5	Incident disclosed by authorities of victim state

4. Start date

Earliest point of target-network access / infiltration / exploitation or the attempt of it.
For example - in case of phishing: The time when the phishing mail actually reached the victim, based on a criminal law argumentation for the attempt to commit a crime (cf. IL basis Art. 25 III lit. F Rome Statute). Crucial for an attempted offense is that there is "action that commences its execution by means of a substantial step".

5. End date

Latest point of target-network access/infiltration/exploitation or the attempt of it.
If public sources suggest that the operation is not yet completed, "na" is coded.

6. Receiver / target category / *multiple codings possible*

Each receiver category, i.e. the categorization of the affected target sectors, is directly assigned the respective receiver countries for each incident. The same applies to the recipient name(s), i.e. the exact designation of the affected target sectors, if this information is publicly available.

Code	Subcode	Description
0		Unknown
1		State institutions / political system
	1	Government / ministries
	2	Legislative
	3	Civil service / administration *(also public schools)*
	4	Judiciary
	5	Military
	6	Police
	7	Intelligence agencies
	8	Political parties
	9	Election infrastructure / related systems
	11	Other (e.g. embassies)
2		International / supranational organisation
3		Critical infrastructure

	1	Energy
	2	Water
	3	Transportation
	4	Health
	5	Chemicals
	6	Telecommunications
	7	Food
	8	Finance
	9	Defence industry
	10	Space
	11	Waste Water Management
	12	Critical Manufacturing
	13	Other
4		Social groups
	1	Ethnic
	2	Religious
	3	Hacktivist
	4	Criminal
	5	Terrorist
	6	Advocacy / activists (e.g. human rights organisations)
	7	Political opposition / dissidents / expats
	8	Other social groups
5		Corporate Targets *(corporate targets only coded if the respective company is no part of the critical infrastructure definition)*
6		End user(s) / specially protected groups (e.g. data subjects, EU consumers)
7		Media
8		Science
9		Other

7. Receiver / target country / *multiple codings possible*

Note: The term “country“ – as applied to the selection list – comprises states, provinces, and territories. This designation does not reflect an official position regarding the status of a given country or region.

8. Receiver regime type / *multiple codings possible*

According to Freedom House “Freedom in the World” report for the respective countries in the respective year. This category can only be coded after the report for the respective starting year of the incident has been published.

Code	**Description**
0	Country unknown
1	Freedom House (respective year) “free”
2	Freedom House (respective year) “partly free”
3	Freedom House (respective year) “not free”

9. Receiver name / *multiple codings possible* **NEW**

Name(s) of the affected receiver(s), e.g. the institutional/corporate/personal name.
In case of multinational corporations, only the name of the parent company is coded.

10. Initiator category / *multiple codings possible*

Categorises the actorness of the attributed attacker for each incident, if available.

Code	Subcode	Description
0		Unknown - not attributed
1		State
2		Non-state actor, state-affiliation suggested
	1	Non-state group, state-affiliation suggested *(widely held view for the attributed initiator (group), but not invoked in this case)*
3		Non-state group
	1	Ethnic actors
	2	Religious actors
	3	Hacktivist(s)
	4	Criminal(s)
	5	Terrorist(s)
	6	Private technology companies / hacking for hire groups without state affiliation / research entities
	7	Other non-state groups
4		Individual hacker(s)
5		Other

11. Initiator country / *multiple codings possible*

The term “country“ – as applied to the selection list – comprises states, provinces, and territories. This designation does not reflect an official position regarding the status of a given country or region.

12. Initiator regime type / *multiple codings possible*

According to Freedom House “Freedom in the World” report for the respective countries in the respective year. This category can only be coded after the report for the respective starting year of the incident has been published.

Code	Description
0	Country Unknown
1	Freedom House (respective year) “free”
2	Freedom House (respective year) “partly free”
3	Freedom House (respective year) “not free”

13. Initiator name / *multiple codings possible*

Name(s) of the initiating group (if known), according to a) their self-declaration (e.g. hacktivist-groups), b) the telemetry of private IT-companies and c) (if available) the designations of aligned offline-state-units, e.g., military unit names.

14. Attribution date

The date of public expression for each coded attribution.

15. Attribution basis / *multiple codings possible*

Code	**Description**
0	Media-based attribution
1	Receiver attributes attacker
2	IT-security community attributes attacker
3	Attacker confirms
4	Contested attribution
5	Attribution by third-party
6	Attribution by receiver government / state entity
7	Attribution by international organisation
8	Attribution by EU institution / agency **NEW**

16. Attribution type / *multiple codings possible*

Code		**Description**
0		Attribution given, type unclear
1		Self-attribution in the course of the attack *(e.g. via defacement statements on websites)*
2		Media report *(e.g. Reuters makes an attribution statement, without naming further sources)*
3		Direct statement in media report (*e.g. Reuters article cites the attribution statements by a person*) / self-attribution via social media
4		Anonymous statement in media report *(e.g. Reuters article cites the attribution statements of unnamed officials, or persons with knowledge into the matter etc.)*
5		Technical report *(e.g. by IT-companies, Citizen Lab, EFF)*
6		Political statement / report *(e.g. on government / state agency websites)*
7		Domestic legal action
	1	Indictment
	2	Sanctions
	3	Arrests
	4	Lawsuit (by private actors)

17. Attribution Country / *multiple codings possible* **NEW**

ISO 3166 ALPHA-3 country codes for the geographic origin(s) of the coded Attribution Bases.

18. Attributing Actor / *multiple codings possible* **NEW**

Name(s) of the attributing actor, e.g. the institutional/corporate/personal name.
In case of multinational corporations, only the name of the parent company is coded.

19. Country of Origin: Proxy / *multiple codings possible* **NEW**

ISO 3166 ALPHA-3 country codes for the geographic origin(s) of the attributed proxy-/state-sponsored actors as initiators.

20. Temporal attribution sequence

Only relevant if Attribution Basis is 2 *(IT-security community attributes attacker)* AND 6 *(attribution by receiver government / state entity)* and / or 8 *(attribution by EU institution / agency).*

Code	Description
0	Temporal attribution sequence unclear
1	Political attribution before IT-security attribution
2	IT-security attribution before political attribution

21. Cyber-conflict issue / *if appropriate, multiple codings possible*

*According to the Conflict Issues by the Conflict Barometer of the Heidelberg Institute for International Conflict Research (HIIK), see https://hiik.de/hiik/methodology/?lang=en.**

Code	Description
0	Unknown
1	System / Ideology
2	National power
3	Autonomy
4	Territory
5	Subnational predominance
6	Resources
7	International power
8	Decolonization
9	Secession
10	Cyber-specific**
11	Other

Remarks:

***The conflict issue "cyber-specific" was added, e.g. for cyber-operations concerning genuinely cyber-related events or issues (example: DDoS-operations by hacktivists against a national court authorizing online-censorship-measures).*

22. Offline-conflict (intensity) - HIIK

According to the intensity levels by the Conflict Barometer of the Heidelberg Institute for International Conflict Research (HIIK), see https://hiik.de/hiik/methodology/?lang=en.

Only relevant for cyber-operations that indicated direct links to the respective HIIK-offline-conflicts. This category can only be coded after the Conflict Barometer for the respective starting year of the incident has been published.

Code	Subcode	Description
0		Unknown
1		Yes / HIIK intensity
	1	HIIK 1
	2	HIIK 2
	3	HIIK 3
	4	HIIK 4
	5	HIIK 5

23. Offline-conflict (issue) - HIIK / *multiple codings possible*

According to the conflict issues by the Conflict Barometer of the Heidelberg Institute for International Conflict Research (HIIK), see https://hiik.de/hiik/methodology/?lang=en.
Only relevant for cyber-operations that indicated direct links to the respective HIIK-offline-conflicts. This category can only be coded after the Conflict Barometer for the respective starting year of the incident has been published.

Code	Description
0	Unknown
1	System/Ideology
2	National power
3	Autonomy
4	Territory
5	Subnational predominance
6	Resources
7	International power
8	Decolonization
9	Secession
10	Other
11	Third-party intervention / Third-party affection*

Remark:
** Additionally coded for cases in which the cyber-attacker conducts its operation because of a specific offline-conflict captured by the HIIK conflict barometer, without being officially part of it (e.g. patriotic hacktivists from one state act in solidarity with another state because of escalating dynamics in the offline-conflict-realm).*

24. Political response date **NEW**

The date of public expression for each coded political response.

25. Political response type **NEW**

Indicates in what form(s) / by which means actors responded to an incident on a political level. Responses find their basis in the instruments of the CFSP.

Code	Subcode	Description
State Actors		
		Outward reactions
1		Preventive measures
	1	Confidence and security-building Dialogues
	2	Capacity building in third countries
	3	Awareness raising
2		Cooperative measures
	1	Demarches
	2	Diplomatic protest notes
3		Stabilizing measures
	1	Statement by minister of foreign affairs
	2	Statement by head of state/head of government
	3	Statement by other ministers/members of parliament
		Inward reactions
4		Legislative reactions
	1	Legislative initiative
	2	Parliamentary investigation committee
5		Executive reactions
	1	Removal from office
	2	Resignation
International organisations		
		Outward reactions
6		Preventive measures
	1	Confidence and security-building Dialogues
	2	Capacity building in third countries
	3	Awareness raising
7		Cooperative measures
	1	Demarches
	2	Protest notes
8		Stabilizing measures
	1	Statement by secretary-general or similar
		Inward reactions
9		Legislative reactions
	1	Legislative initiative
	2	Parliamentary investigation committee
10		Executive reactions
	1	Removal from office
	2	Resignation
EU		
		Outward reactions
11		Preventive measures
	1	Confidence and security-building Dialogues
	2	Capacity building in third countries
	3	Awareness raising
12		Cooperative measures
	1	EU demarches
	2	Diplomatic protest notes
13		Stabilizing measures
	1	Common Position of the European Council
	2	CFSP Conclusions
	3	CFSP Decisions
	4	Statements by HR on behalf of the Council

	5	Declaration of HR
		Inward reactions
14		Legislative reactions
	1	Legislative initiative
	2	Parliamentary investigation committee
15		Executive reactions
	1	Removal from office
	2	Resignation
EU member states		
		Outward reactions
16		Preventive measures
	1	Confidence and security-building Dialogues
	2	Capacity building in third countries
	3	Awareness raising
17		Cooperative measures
	1 2	Demarches Diplomatic protest notes
18	 1 2 3	Stabilizing measures Statements by foreign ministers Statements by heads of state Statement by other ministers/members of parliament
		Inward reactions
19		Legislative reactions
	1	Legislative initiative
	2	Parliamentary investigation committee
20		Executive reactions
	1	Removal from office
	2	Resignation

26. Political response country **NEW**

ISO 3166 ALPHA-3 country codes for the geographic origin(s) of the politically responding actors.

27. Political response actor **NEW**

Name(s) of the politically responding institutions / entities / actors.

28. Zero day(s)

Code	Subcode	Description
0		Unknown
1		No
2		Yes
	1	One
	2	Multiple

29. MITRE: Initial Access **NEW**

Describes the entry vectors that are used by attackers in order to gain initial foothold within the target networks, according to MITRE ATT&CK framework.
For further information please see https://attack.mitre.org/tactics/TA0001/.

Code	Description
1	Drive-By Compromise
2	Exploit Public-Facing Application
3	External Remote Services
4	Hardware Additions
5	Phishing
6	Replication Through Removable Media
7	Supply Chain Compromise
8	Trusted Relationship
9	Valid Accounts

30. MITRE: Impact **NEW**

Describes the actual impact an attacker causes within the target networks, according to MITRE ATT&CK framework.
For further information please see https://attack.mitre.org/tactics/TA0040/.

Code	Description
1	Account Access Removal
2	Data Exfiltration **NOT INCLUDED BY MITRE**
3	Data Destruction
4	Data Encrypted for Impact
5	Data Manipulation
6	Defacement
7	Disk Wipe
8	Endpoint Denial of Service
9	Firmware Corruption
10	Inhibit System Recovery
11	Network Denial of Service
12	Resource Hijacking
13	Service Stop
14	System Shutdown/Reboot

31. CVSS: User Interaction **NEW**

Describes if an incident needs user interaction in order to be successful, according to the framework of the Common Vulnerability Scoring System, category “User Interaction”.
For further information please see https://www.first.org/cvss/specification-document.

Code	Description
1	None
2	Required

32. Incident type(s) / *multiple codings possible*

Code	Subcode	Description
1		Data theft / Data loss
	1	Combined with doxing
2		Disruption
3		Hijacking with misuse
4		Hijacking without misuse
5		Ransomware

Remark:
The incident type "ransomware" is always coded in conjunction with one or more of the other incident types, according to the type of ransomware given (e.g. "classic" ransomware vs. double or triple extortion). Therefore, the code "ransomware" serves as an additionally specifying incident type label.

Intensity based on incident types

Note: Since ransomware incidents are coded as a combination of the other incident types as well, their intensity score also builds on their intensity coding. Thus, ransomware is not listed as a separate category below.

33. Data theft

Code	Description
0	None
1	For political / military targets: non-classified information *(incident scores 1 point in intensity)* For private / commercial targets: non-sensitive information *(incident scores 1 point in intensity)*
2	For political / military targets: classified information *(incident scores 2 points in intensity)* For private / commercial targets: sensitive information *(incident scores 2 points in intensity)*

Remark:
If public sources do not explicitly designate the information involved as "classified" or "sensitive," the intensity of data theft is coded 1.

34. Disruption

Code	Description
0	None
1	Short-term disruption *(< 24h; incident scores 1 point in intensity)*
2	Long-term disruption *(> 24h; incident scores 2 points in intensity)*

Remark:
The disruption needs to be caused directly by the respective cyber operation. Disruptions caused by precautionary measures are not included here.

35. Hijacking (accessing and controlling a system)

Code	Description
0	None
1	Hijacking, not used - empowerment *(incident scores 1 point in intensity)*
2	Hijacking, system misuse, e.g., through data theft and / or disruption *(incident scores 2 points in intensity)*

Remark:

Hijacking without misuse means the infiltration/compromise of targeted systems, e.g. via gaining a foothold in its networks, without obviously misusing these privileges. It is usually conducted by using malware, such as Remote Access Trojans.

36. Physical effects (spatial)

Code	Description
0	None
1	Local effects, e.g. affecting only one restricted area of a country or region *(incident scores 1 point in intensity*)
2	Widespread effects, e.g. affecting different regions of country or a country as a whole *(incident scores 2 points in intensity)*

37. Physical effects (temporal)

Code	Description
0	None
1	Short duration *(< 24h; incident scores 1 point in intensity)*
2	Long lasting effects *(> 24h; incident scores 2 points in intensity)*

38. Unweighted cyber intensity

Sum of data theft + disruption + hijacking + physical effects spatial + physical effects temporal = maximum score 10

39. Target / effect multiplier

Code	Description
1	Moderate - high political importance
2	Very high political importance (e.g. critical infrastructure, military) - intensity multiplied by 1.5

The 1.5 multiplier is applied based on societal effects. It is only applied, when there is a widespread disruption of services that are of critical importance for the functioning of affected societies. In case of the military the respective social function (national defence) has to be affected, the same applies to critical infrastructures. Other attacks on critical infrastructure / military entities are multiplied by 1.0.

40. Weighted cyber intensity

Unweighted cyber intensity multiplied with target multiplier / *brought up to round figure*

1	Low / Moderate intensity
2	
3	
4	
5	
6	High intensity
7	
8	
9	
10	
11	Very high intensity
12	
13	
14	
15	

41. Impact Indicator: Total Score **NEW**

The overall impact indicator score is automatically created based on the sum of the coding for its five sub-indicators (see below). Sub-indicators derive from Impact Assessment in Art. 3 Decision (GASP) 2019/797.

Example: An incident is rated 1, 3, 2, 4, and 1 for the sub-indicators, which adds up to 11, i.e. a "medium impact."

Code	**Description**
1 *(sum of sub-scores 1 – 5)*	Minor
2 *(sum of sub-scores 6 – 10)*	Low
3 *(sum of sub-scores 11 – 15)*	Medium
4 *(sum of sub-scores 16 – 20)*	High
5 *(sum of sub-scores 21 – 25)*	Very High

42. Impact Indicator: Sub-Indicator “Economic Impact” **NEW**

Refers to the total economic / financial loss an incident or campaign causes to the affected targets as a whole. The ranges are drawn from empirical evidence for usual revenue operations. Thus, incidents with only one or few targets will most likely be scored 2, especially if they are no typical revenue operations. It can be coded for EURO or US-Dollar.

Code	**Description**
1	None
2	=< 10 Mio
3	> 10 Mio – 100 Mio
4	> 100 Mio – 1 Bn
5	> 1 Bn

43. Impact Indicator: Sub-Indicator “Political Impact” (affected entities) **NEW**

Indicates the number of affected EU-organizations / entities / actors OR Third Country-organizations / entities / actors.

Code	Description
1	1 - 10
2	11 - 50
3	51 - 200
4	201 - 500
5	50 1 – 10.000 (or more)

44.A Impact Indicator: Sub-Indicator “Political Impact (EU-Countries)” **NEW**

Indicates the number of affected EU-member states *(will be coded for incidents with EU-member states among the coded receiver countries even if there are additionally third countries among the receiver countries).*

Code	Description
1	1 - 5
2	6 - 10
3	11 - 15
4	16 - 20
5	21 - 27

44. B Impact Indicator: Sub-Indicator “Political Impact (Third Countries)” **NEW**

Indicates the number of affected Third Countries (incidents without affected EU-member states) *(will be coded instead of "Political Impact (EU-Countries)" for incidents that do not have EU-member states among the coded receiver countries).*

Code	Description
1	1 - 10
2	11 - 20
3	21 - 50
4	51 - 100
5	101 - 193

45. Impact Indicator: Sub-Indicator “Intelligence Impact” **NEW**

Indicates the criticality of data exfiltration / corruption.

Code	Description
1	No data breach / exfiltration or data corruption (deletion / altering) and / or leaking of data
2	Minor data breach / exfiltration (no critical / sensitive information), but no data corruption (deletion / altering) or leaking of data
3	Data corruption (deletion / altering) but no leaking of data, no data breach / exfiltration OR major data breach / exfiltration, but no data corruption and / or leaking of data
4	Minor data breach / exfiltration (no critical / sensitive information), data corruption (deletion / altering) and / or leaking of data
5	Major data breach / exfiltration (critical / sensitive information) & data corruption (deletion / altering) and / or leaking of data

Explanation:

Code	Minor Data Breach/Exfiltration *(no critical/ sensitive information)*	Major Data Breach/Exfiltration *(critical/sensitive information)*	Leaking of Data	Data Corruption *(manipulation, encryption, deletion)*
1	-	-	-	-
2	x	-	-	-
3	-	-	-	x
	-	x	-	-
4	x	-	x	-
	x	-	-	x
	x	-	x	x
5	-	x	x	-
	-	x	-	x
	-	x	x	x

46. Impact Indicator: Sub-Indicator "Functional Impact" **NEW**

Indicates the time period in which a functionality of the target systems was affected.

Code	Description
1	No system interference / disruption
2	Day (< 24h)
3	Days (< 7 days)
4	Weeks (< 4 weeks)
5	Months

47. State Responsibility Indicator **NEW**

Indicates the degree of state-responsibility (based on ILA's Articles of State Responsibility) for an incident / operation.

Code	Description
1	None / Negligent
2	Indirect (knowingly sanctioning / ordering / ideological / material support by official members of state entities / agencies / units for officially non-state actors)
3	Direct (official members of state entities / agencies / units responsible)

48. International Law Breach Indicator **NEW**

Indicates the areas of international law that have been affected / violated.

Code	Subcode	Description
1		Cyber espionage
	1	State actors
	2	Non-state actors
2		Human rights
	1	Civic / Political rights
	2	Economic, social and cultural rights

	3	Other human rights instruments
3		Diplomatic / Consular law
4		Air law
5		Law of the sea
6		Space law
7		International telecommunication law
8		International peace
	1	Peaceful settlement
	2	Prohibition of intervention
	3	Use of force
9		Armed conflict
	1	Conduct of hostilities
	2	Certain persons
	3	Occupation
	4	Neutrality
10		Due diligence
11		Sovereignty
12		Law of treaties (pacta sunt servanda)
13		Good faith
14		Self-determination
15		International criminal law
16		Aid and development
17		Disaster management
18		International economic law
19		Intellectual property law
20		International organizations
21		Other

49. Evidence for sanctions indicator **NEW (upcoming)**

Indicates the level of publicly available evidence that would justify the imposition of different forms of sanctions.

Code	Description
1	Low
2	Medium
3	High

50. Response indicator **NEW**

Indicates if and what (legal) response options are justified, based on publicly available information.

Code	Description
1	No response justified *(missing state attribution & breach of international law)*
2	Unfriendly acts / retorsions justified *(missing state-attribution & breach of international law OR state-attribution & missing breach of international law)*
3	Countermeasures under international law justified *(state-atttribution & breach of international law)*

51. Legal response date **NEW**

The date of public expression for each coded legal response.

52. Legal response type **NEW**

Indicates in what form(s) / by which means actors responded to an incident on a legal level. Examples of Retorsions are derived from T Giegerich, 'Retorsion' (last updated September 2020) in A Peters and R Wolfrum (eds), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press 2008–) <www.mpepil.com> (accessed 14 September 2022).

Code	Subcode	Description
1		Peaceful means: Retorsion (International law)
	1	Expulsion of diplomatic staff
	2	Severance of diplomatic relations
	3	Travel bans
	4	Economic sanctions
	5	Other Acts of Retorsion
2		Reprisal / Countermeasures (Art. 22, 49-54 ASR)
3		Use of force (International Law)
	1	Self-defence (Art. 21 ASR, Art. 51 UN Charter)
	2	Art. 41 UN Charter
	3	Art. 42 UN Charter
	4	Art. 4 North Atlantic Treaty
	5	Art. 5 North Atlantic Treaty
4		No justification under IL
5		Restrictive measures (Art. 215 TFEU/Title V Chapter 2 TEU)
	1	Restrictive measures against countries (Art. 215 (1) TFEU)
	2	Restrictive measures against individuals (Art. 215 (2) TFEU)
6		Solidarity clause (Art. 222 TFEU)
7		Collective regional self-defence (Art. 42 (7) TEU)
8		Proclamation of public emergency
9		Other legal measures on national level (e.g. law enforcement investigations, arrests)

53. Legal response country **NEW**

ISO 3166 ALPHA-3 country codes for the geographic origin(s) of the legally responding actors.

54. Legal response actor **NEW**

Name(s) of the legally responding institutions/entities/actors.

55. Legal attribution reference **NEW**

Indicates the area of international law that is referred to by an attributing actor.

Code	Subcode	Description
1		Cyber espionage

	1	State actors
	2	Non-state actors
2		Human rights
	1	Civic / Political rights
	2	Economic, social and cultural rights
	3	Other human rights instruments
3		Diplomatic / Consular law
4		Air law
5		Law of the sea
6		Space law
7		International telecommunication law
8		International peace
	1	Peaceful settlement
	2	Prohibition of intervention
	3	Use of force
9		Armed conflict
	1	Conduct of hostilities
	2	Certain persons
	3	Occupation
	4	Neutrality
10		Due diligence
11		Sovereignty
12		Law of treaties (pacta sunt servanda)
13		Good faith
14		Self-determination
15		International criminal law
16		Aid and development
17		Disaster management
18		International economic law
19		Intellectual property law
20		International organizations
21		Other

56. Casualties

Code	**Description**
0	No casualties as a direct result of the cyber incident
1	Injured (incident gets marked as category A)
2	< 25 (incident gets marked as category B)
3	>= 25 (incident gets marked as category C)

57. Sources

URLs

58. Sources attribution

URLs

59. Sources politicization

URLs

60. Incident name

All incidents that were reported before 2022: Denominator that is mostly used to refer to the respective incident (e.g., Stuxnet), else descriptive denominator (e.g. Ukraine power outage 2015).

Naming convention for incidents reported since 2022:

[Malware/ Initiator Name] [Action] [Receiver Country] [Target/ Target Sector] [Start Year]

61. Description

Short description of the incident.

Building blocks:

[Context/ Operation Name if distinct:] [Confidence Qualifier] [Initiator Country] [Initiator Name/Descriptor] [Action] [Receiver Country] [Target/ Target Sector] [Objective] [Start and End Date] [According to Settled Attribution: Attribution Actor]