UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

# A Taxonomy of Malicious ICT Incidents

## INTRODUCTION

The international community is expressing growing concerns regarding existing and potential threats in the sphere of information communication technology (ICT) security.[1] The first final substantive report by the United Nations Open-ended working group (OEWG) on developments in the field of information and telecommunications in the context of international security, highlighted that "[h]armful ICT incidents are increasing in frequency and sophistication, and are constantly evolving and diversifying".[2] Member States have also acknowledged that the threat landscape varies by region and State and that what constitutes a threat varies according to each country's characteristics. However, despite pointing to the deterioration of the ICT security environment, the United Nations cyber processes have not focused on mapping a common threat landscape.

One of the reasons for the lack of a shared characterization of the threat environment at the multilateral level is the absence of consensus and clarity in describing the threats. This lacuna originates from multiple factors. First, there is a gap in common standards in the public and private sectors on how to categorize and measure cyber incidents.[3] Second, some existing taxonomies are too technical and too detailed to be consulted and used by non-ICT experts or practitioners. While relevant for subject experts' assessments, such technicalities and details may hinder discussions at the political or strategic level. Third, some taxonomies employ concepts that are highly contested by some Member States, such as 'threat actor' or 'cyber attack', or they refer to actions that are not considered inconsistent with their obligations under the framework of responsible State behaviour. Therefore, these terms are not conducive for discussions in international multilateral forums.

This research project proposes a taxonomy of malicious ICT incidents that can be used to analyse ICT events both in peace and conflict settings, and that is suitable for international multilateral discussions. Indeed, it is aimed at fostering a common understanding and baseline knowledge to analyse the cyber threat landscape. The use of a shared taxonomy may further advance Member States' discussions in the ongoing United Nations process, namely the OEWG, and it may provide the international community with a tool to facilitate information-sharing and thus confidence-building.

## THE STRUCTURE AND HOW TO READ THE TAXONOMY

The taxonomy of malicious ICT incidents presented here is composed of a simple radial diagram (see figure). In the left section, there are the elements or inputs necessary for a malicious ICT incident to take place. These are the perpetrator, the vector, the victim, the targeted asset, and the cybersecurity failures. At the center of the radial diagram, there is the malicious ICT act, which refers to the intentional act that leverages ICTs to compromise the confidentiality, integrity, and availability of data. On the right part of the infographic, there are the possible outputs resulting from the malicious ICT act.

This taxonomy uses the terms 'incident' and 'act' in two distinct ways. The first refers to the broader understanding of a malicious ICT event, which encompasses all the elements identified in the taxonomy. The second refers directly to the penetration or hacking of a system or a network.

Each cell of the radial diagram focuses on a specific component of the incident that helps to identify and to categorize it. The cells have been created drawing on a review of the existing technical literature and interviews with ICT experts. Within the categories, additional items are listed to help the reader to further identify the specifics of each element. The list is not be considered closed, rather new typologies of items can be included as needed. In the following paragraphs, each of the taxonomy components is explained.

## INPUT CELLS

The **input cells**, identified by outgoing arrows, represent key elements that are necessary for the realization of a malicious ICT incident.

### Perpetrator

The perpetrator can be a person or an entity that carries out a malicious act against a victim. This taxonomy identifies the following possible actors:

- **State actors**
- **Non-State actors**

Both categories include more detailed subcategories.

For State actors, the subcategories are drawn from the customary law of State responsibility. They are:

- *de jure* State organs, irrespective of their hierarchical position in the apparatus of the State or the constitutional structure or organization of the State;[4]
- *de facto* State organs, referring to "non-State actors or entities that have been 'elevated' to *de facto* State agents or organs";[5] and
- entities controlled or directed by a State, that is, individuals or groups over which a State exercises 'effective control'.[6]

---

1 United Nations General Assembly. 2021a. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN document A/76/135; United Nations General Assembly. 2021b. Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/75/816.

2 United Nations General Assembly. 2021b. para. 15

3 Charles Harry and Nancy Gallagher. 2018. "Classifying Cyber Events." Journal of Information Warfare, vol. 17, no. 3 (2018), pp. 17–31, p. 17.

4 Constantine Antonopoulos. 2021. "State Responsibility in Cyberspace." In: Nicholas Tsagourias and Russel Buchan (eds.) Research Handbook on International Law and Cyberspace. p. 116.

5 Ibid.

6 Ibid.

Non-State actors are:
– individuals or groups, that is, any natural person that is conducting malicious activities alone or in a group; and
– organizations, being any entity recognized by a State (private companies, associations, non-governmental organizations, etc..).

### Targeted Asset

Within the victims' ICT environment, there are specific assets that may be targeted by a malicious act. Throughout the penetration phase, the perpetrator might go through different assets to achieve the objective of the act. This taxonomy relies on the classification of targets conceptualized by Simmons et al.,[7] and it is composed of the following elements:

- **operating system (OS)**: a malicious act can target specific vulnerabilities in an OS;
- **network**: the malicious act targets a particular network of devices, which can range from a local area network (LAN) to an industrial control system (ICS), or networks of networks, such as a metropolitan area network (MAN);
- **local device**: usually refers to a user's local device (such as personal computer, or smartphone);
- **user**: the person that uses ICTs—in this case, the perpetrator targets the user to retrieve personal information; and
- **application**: an application is either client or server, with a client application being software that is running on a user's local device, whereas a server application is software running on a remote device.

### Vector

The vector, or attack vector, refers to the means by which the perpetrator is able "to gain access to information resources or system".[8] This taxonomy relies on the further categorization carried out by Scott D. Applegate and Angelos Stavrou,[9] which includes:

- **technology**: the perpetrator exploits or manipulates technology, such as exploiting ICT vulnerabilities;
- **process**: access is gained by manipulating flawed processes, which could be organizational (such as security policies) or production (such as supply chain); and
- **people**: the perpetrator manipulates people (e.g., social engineering) to access systems or networks.

To carry out a malicious act, the perpetrator may use multiple vectors.

### Victim

Each malicious ICT incident may affect a subject or a number of subjects, depending on how targeted or controlled the malicious act is. This taxonomy breaks down the victim analysis into **three main subcategories**:[10]

- **intended victim**: the intended victim of a malicious act;
- **instrumental victim**: the subject exploited by the perpetrator to achieve or leverage an effect on the intended victim (e.g. an unaware person whose device is part of a botnet to conduct an attack on the intended victim); and
- **collateral victims**: the subjects unintentionally involved in a malicious ICT incident (e.g. organizations hit by the uncontrolled propagation of a worm).

Victims may range from a single user to the critical infrastructure of a State. For analytical purposes, victims can be categorized into:

- **individuals** (such as CEOs, users, citizens, political leaders, or celebrities);
- **organizations** (such as companies, universities, political parties, or non-governmental organizations);
- **critical infrastructure/property** (such as transport, energy, health, Internet of Things, etc.);[11]
- **countries** (such as their economy, security, society as a whole, political system, etc.); and
- **the international system** (such as international organizations, regional entities, or the environment).

### Cybersecurity Failures

The success of a malicious ICT act depends not only on the perpetrator's knowledge and capabilities but also on the cybersecurity preparedness of the victim. This taxonomy adopts a wide understanding of cybersecurity failures, which concern both ICT and human-related elements. These are classified into four main categories:

- **ICT defence and monitoring**;
- **product vulnerabilities**;
- **organizational failures**; and
- **human failures**.

ICT defence and monitoring pertain to the ICT dimension of cybersecurity and can be further unpacked into two subcategories.

– ICT defence, which could be active or passive.[12] In general, it refers to protection measures deployed to protect a system or a network (e.g. honeypots or firewalls).
– monitoring, which refers to the constant activity of scrutinizing network traffic and endpoints. This helps to spot anomalous activities before they can produce disruptive or exploitative effects.

---

[7] Chris Simmons, et al. 2009. "AVOIDIT: A Cyber Attack Taxonomy." Technical Report, University of Memphis, Number CS-09-003.
[8] Scott D. Applegate and Angelos Stavrou. 2013. "Toward a Cyber Conflict Taxonomy". 5th International Conference on Cyber Conflict (CYCON 2013), pp. 1–18. p. 7.
[9] Ibid.
[10] In case of an armed conflict, this taxonomy does not differentiate the victims of a malicious act in terms of *legitimate* or *illegitimate*.
[11] Ioannis Agrafiotis, et al. 2016. "Cyber Harm: Concepts, Taxonomy and Measurement" (August 1, 2016). Saïd Business School WP 2016-23.
[12] Scott D. Applegate and Angelos Stavrou. 2013. "Toward a Cyber Conflict Taxonomy". 5th International Conference on Cyber Conflict (CYCON 2013), pp. 1–18. p. 7.
[13] In this case, if a vulnerability can be found by an external actor, it becomes a 'zero day' vulnerability (referring to the number of days the producer is aware of it).

Another ICT dimension of cybersecurity is the existence of product vulnerabilities.

– ICT products and services may have flaws or vulnerabilities that have not been discovered[13] or patched yet by the producer or vendor (or not installed by the user). Such vulnerabilities can be exploited for malicious purposes.

Beyond ICT-related failures, there are also human-based failures, which refer to organizational and human elements.

– organizational. Legal entities may have organizational policies/practices concerning cybersecurity. For example, setting up a cybersecurity perimeter or creating a Computer Emergency Response Team could help to deter a malicious cyber act. Unfortunately, not all entities set up or define these policies/practices; moreover, there might be flaws in their conceptualization or implementation phases that could allow the perpetrator to succeed in penetrating the network or the system.
– human. Perpetrators often leverage the human element for their malicious purposes.[14] Indeed, humans are the most vulnerable link of the cybersecurity chain. Each of us can consciously or unconsciously provide important information to a malicious actor or facilitate perpetrators' efforts to penetrate our devices/accounts. For example, a lack of awareness of basic cyber hygiene practices can be conducive to malicious activities.

## THE MALICIOUS ICT ACT CELL

A **malicious ICT act** is conceptualized as an intentional act that leverages ICTs to compromise the confidentiality, integrity, and availability of data producing disruptive effects on a victim.[15] This taxonomy does not consider non-adversarial accidents or failures, which, for example, can be the results of environmental events.

The malicious act can be broken down into more specific steps, which range from analysing the different operational objectives[16] to looking at the different tactics, techniques, and procedures[17] used throughout the different stages of the so-called cyber 'kill chain'.[18] However, these analyses are outside the scope of this taxonomy.

## OUTPUT CELLS

The **output cells**, identified by incoming arrows, refer to key elements that may occur as a result of a malicious ICT act.

### Effect

Each cyber incident produces an effect on a target.[19] There are two main types of primary effects resulting from a malicious ICT act: disruptive and exploitative.[20] As noted in fn. 15 above, this taxonomy looks only at acts that produce disruptive effects.

Disruptive effects are produced by malicious activities that interfere with the target's ICT functions, and they can be categorized into four subcategories:

– message manipulation, which refers to effects that alter communication through ICTs. For example, manipulation can take the form of website defacement or hijacking of social media accounts;
– disruption of service, which refers to effects that degrade or deny the victim's ability to access information systems, devices, or other network resources;
– data attack, which refers to acts that produce effects on data, such as data manipulation, destruction, or encryption; and
– destruction, which refers to the disruption of physical systems through ICT manipulation.

### Gains

Behind a malicious ICT incident, there are possible gains that the perpetrator would like to achieve. Gains, therefore, concern the reasons for which an actor is undertaking a malicious ICT act. This taxonomy identifies three categories of gains:

- **political/governmental**: when the gain for the act concerns the political/governmental realm, broadly understood (including military gains, such as operational or tactical advantages that may be achieved through an ICT activity);
- **economic**: including all activities that seek economic or financial gains (including business or criminal gains); and
- **personal**: when malicious activities are driven by personal gains (such as learning or revenge).

### Harm

This taxonomy adopts the following definition of cyber harm, which is the damage directly caused by a malicious act "conducted wholly or partially via digital infrastructures, and the information, devices and software applications that these infrastructures are composed of".[21] Accordingly, there are different categories of harm:[22]

- **physical**: refers to physical or digital damage to someone or something (such as unavailable systems or corrupted data files);
- **psychological/emotional harm**: affects individuals and their mental well-being and psyche. It is the most common harm following a malicious ICT act;
- **economic harm**:[23] refers to economic or financial losses caused by a malicious cyber act and can affect individuals, organizations, and countries alike (such as stealing of credit card credentials, or disruption of business);
- **political and governmental**: encompasses a range of effects on the government, the political system, and its processes (in this subcategory, we included military harm, such as operational or tactical losses incurred from a malicious ICT act);

- **reputational harm**: refers to the harm pertaining to the general opinion held about an entity or a person (such as a damaged public perception, or media scrutiny);
- **cultural**: refers to damage that affects autonomy, development and growth, and access to cultural, intellectual. informational resources of a given society.

### Attribution

Attribution is the process of allocating responsibility for a malicious ICT incident to a natural person or to a legal entity and "it involves the determination of the origin or authorship of the cyber operation".[24] It is comprised of three distinct and intertwined typologies: technical, legal, and political.[25]

- **technical**: implies the analysis of the technical aspects of a malicious ICT incident, which can include malware signatures; tactics, techniques, and procedures (TTP); and traffic analysis. Technical analysis is frequently augmented by the analysis of sociopolitical factors of the malicious ICT incident.
- **legal**: can refer to
  - the responsibility of a State for the conduct of a malicious ICT activity. Not all acts envisage legal considerations as they may not amount to a breach of international obligations of States;[26] and
  - the responsibility of an individual for the conduct of a malicious ICT act, in accordance with domestic legislation and relevant standards of proof.
- **political**: concerns the choice of the victim State to attribute an act to a perpetrator. The political attribution can be private or public. This is a political choice because there are no obligations or expectations for a State to attribute a malicious ICT incident. However, there are a growing number of cases in which States resort to criminal law considerations to politically attribute a malicious incident.[27]

---

[14] Tim Conkle. 2020. **"**The Human Element Of Cybersecurity.**"** Forbes, Jan 24, 2020. Available at: https://www.forbes.com/sites/forbestechcouncil/2020/01/24/the-human-element-of-cybersecurity/?sh=3ecf7dfd3293.

[15] The taxonomy acknowledges the existence of another type of malicious activity that seeks to steal information through the exploitation of different sources. However, because these activities may fall within activities that are not inconsistent with their obligations under the responsible State behaviour framework (which includes voluntary norms, international law, and confidence-building measures), the research does not include them in the taxonomy presented here.

[16] Chris Simmons, et al. 2009. **"**AVOIDIT: A Cyber Attack Taxonomy.**"** Technical Report, University of Memphis, Number CS-09-003.

[17] MITRE. 2015-2022. MITRE ATT&CK. available at: https://attack.mitre.org.

[18] Eric M. Hutchins, Michael J. Cloppert, and Amin M. Rohan. 2011. **"**Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.**"** Lockheed Martin.

[19] Charles Harry and Nancy Gallagher. 2018. **"**Classifying Cyber Events.**"** Journal of Information Warfare, vol. 17, no. 3 (2018), pp. 17**–**31, p. 17.

[20] Ibid.

[21] Ioannis Agrafiotis et al. 2018. **"**A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate**"**. Journal of Cybersecurity, vol. 4, no. 1, 2018.

[22] Ibid.; and Ioannis Agrafiotis, et al. 2016. **"**Cyber Harm: Concepts, Taxonomy and Measurement**"** (August 1, 2016). Saïd Business School WP 2016**–**23.

[23] As argued by Agrafiotis et al., **"**Harm types are designed to be distinctive, however, all types may be attempted to be interpreted in economic terms. Thus, economic harm may overlap with other harm types**"**; Ioannis Agrafiotis et al. 2018. **"**A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate**"**. Journal of Cybersecurity, vol. 4, no. 1, 2018, p. 7.

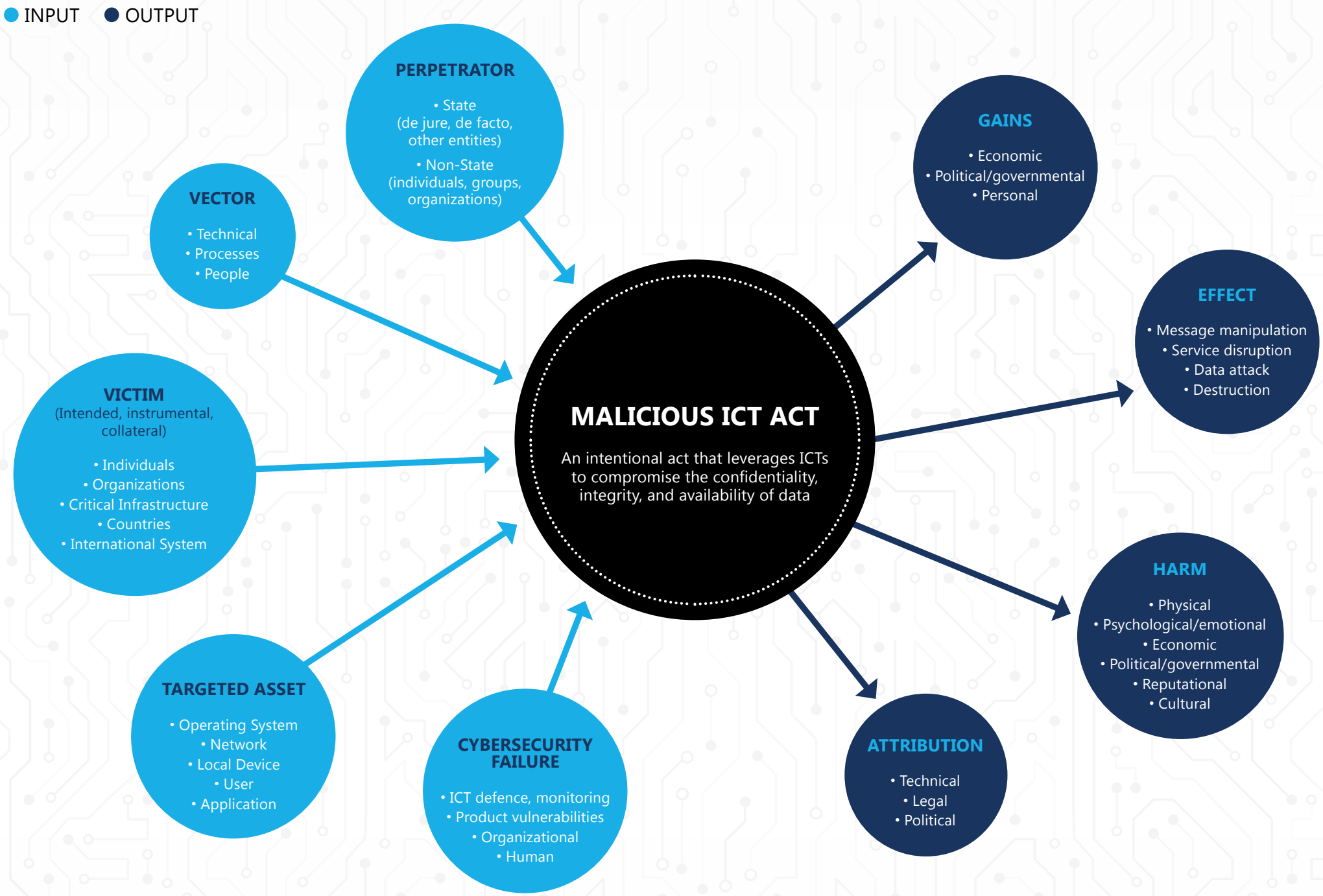
[24] Andraz Kastelic. 2022. Non-Escalatory Attribution of International Cyber Incidents Facts, International Law and Politics. United Nations Institute for Disarmament Research. p. 5.

[25] Ibid.

[26] Ibid., p. 11.

[27] Dennis Broeders, Els De Busser, and Patryk Pawlak. 2020. **"**Three Tales of Attribution in Cyberspace: Criminal Law, International Law and Policy Debates**"**. The Hague Program for Cyber Norms Policy Brief.

# UNIDIR TAXONOMY OF MALICIOUS ICT INCIDENTS



## About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

## Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members, or sponsors.

**www.unidir.org**

@unidirgeneva

@UNIDIR

un_disarmresearch

**Authors:** Samuele Dominioni, Giacomo Persi Paoli

**Support** from UNIDIR core funders provides the foundation for all of the Institute's activities. This study was produced by UNIDIR's Security and Technology Programme, which is funded by the Governments of France, Germany, the Netherlands, Norway, and Switzerland, and by Microsoft. The authors wish to thank the following individuals for their invaluable advice and assistance on this report: Alisha Anand (UNIDIR), Andraz Kastelic (UNIDIR), Moliehi Makumane (UNIDIR), Wenting He (UNIDIR), David Fairchild (Canada), Marie Humeau (the Netherlands), Ivan Kwiatkowski and Anastasiya Kazakova (Kaspersky), Erika Kawahara (UNODA), Alexis Dorais-Joncas (Proofpoint), Stefano Zanero (Politecnico di Milano), and Jinghua Lyu (Center for Humanitarian Dialogue).

**Design:** Kathleen Morf, www.kathleenmorf.ch
**Photos:** Shutterstock. Front/Back Cover: © Immersion Imagery, Inside pages: your, ArtHead