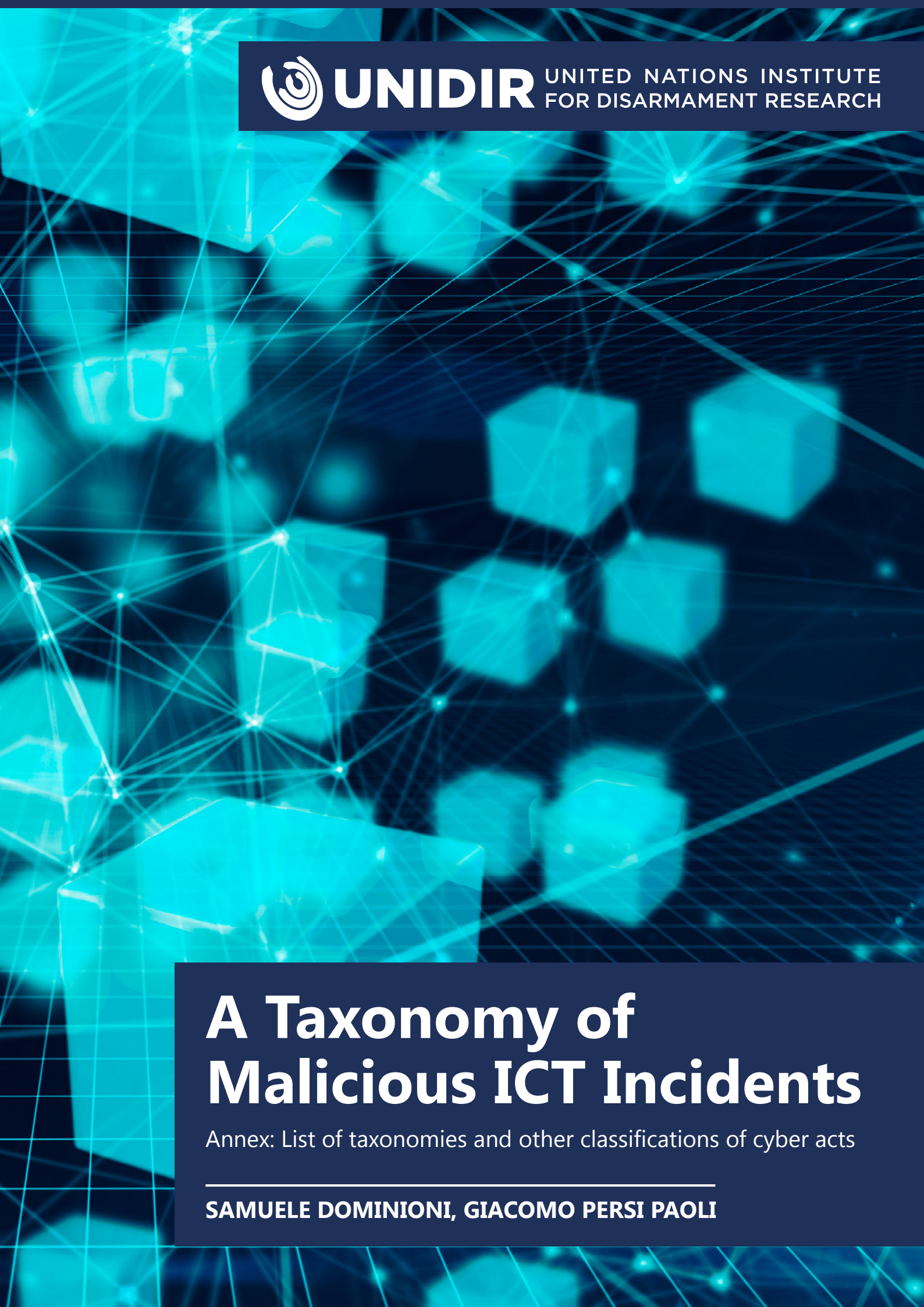


UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

A Taxonomy of Malicious ICT Incidents

Annex: List of taxonomies and other classifications of cyber acts

SAMUELE DOMINIONI, GIACOMO PERSI PAOLI

Acknowledgements

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 the Czech Republic, France, Germany, Italy, the Netherlands, Norway, and Switzerland, and by Microsoft.

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.

The Authors

Dr. Samuele Dominioni is a researcher in the Security and Technology Programme at UNIDIR. Before joining UNIDIR, he held research positions in both academic and think tank settings. He holds a PhD in international relations and political history from Sciences Po, France, and the IMT School for Advanced Studies, Italy.

Dr. Giacomo Persi Paoli is the Head of the Security and Technology Programme at UNIDIR. His expertise spans the science and technology domain with emphasis on the implications of emerging technologies for security and defence. Before joining UNIDIR, Giacomo was Associate Director at RAND Europe where he led the defence and security science, technology and innovation portfolio as well as RAND's Centre for Futures and Foresight Studies. He holds a PhD in economics from the University of Rome, Italy, and a Master's degree in political science from the University of Pisa, Italy.

www.unidir.org | © UNIDIR 2022

Photos: © Shutterstock: Immersion Imagery, your.

TABLE OF CONTENTS

INTRODUCTION 1

THE VECTOR 2

Scott D. Applegate and Angelos Stavrou. 2013. "Toward a Cyber Conflict Taxonomy". 5th International Conference on Cyber Conflict (CYCON 2013), pp. 1–18. 2

THE TARGETED ASSET 4

Chris Simmons et al. 2009. "AVOIDIT : A Cyber Attack Taxonomy." Technical Report, University of Memphis, Number CS-09-003. 4

THE MALICIOUS ICT ACT 6

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. 6

MITRE. 2015–2022. MITRE ATT&CK. 8

THE EFFECT 10

Charles Harry and Nancy Gallagher. 2018. "Classifying Cyber Events". Journal of Information Warfare, vol. 17, no. 3, pp. 17–31. 10

THE HARM AND THE VICTIM 12

Ioannis Agrafiotis et al. 2016. "Cyber Harm: Concepts, Taxonomy and Measurement" (August 1, 2016). Saïd Business School WP 2016-23. 12



INTRODUCTION

The infographic **"A Taxonomy of Malicious ICT Incidents"** relies and builds on several existing taxonomies and classifications concerning different aspects of a malicious ICT event. This annex offers additional information about the sources included in the infographic. In particular, the annex offers:

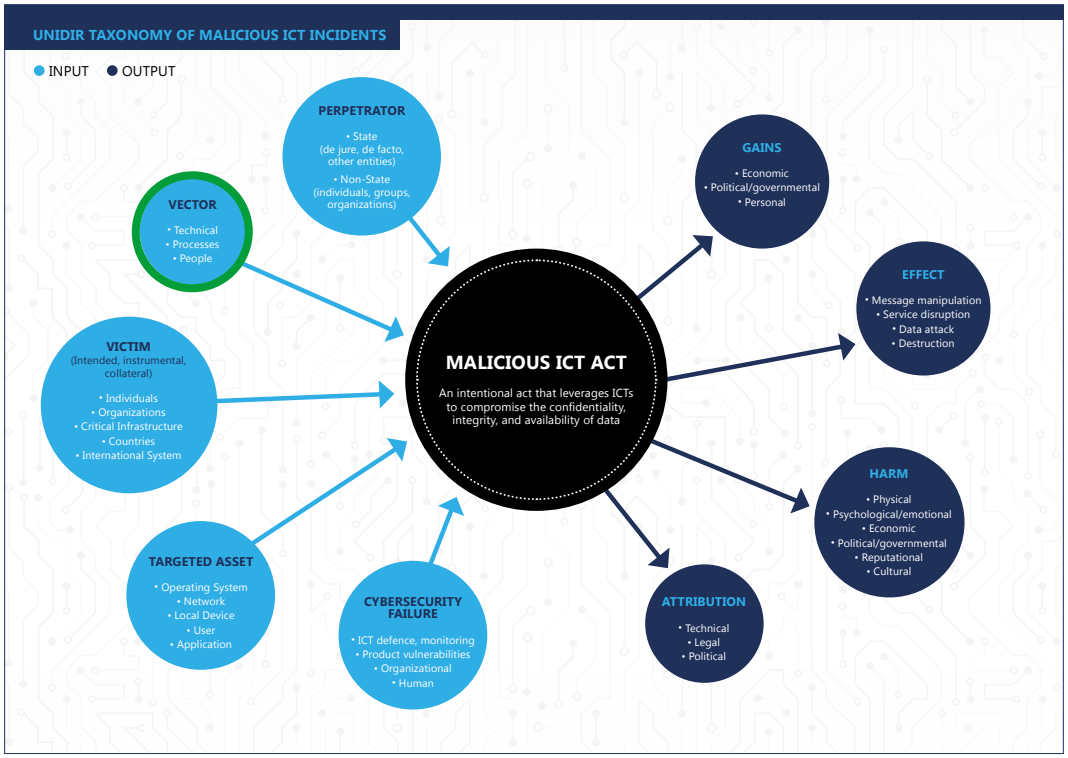
1. a reference (text and image) on how the source has been used in "A Taxonomy of Malicious ICT Incidents";
2. a brief explanation of each of the taxonomies/categorizations quoted in the infographic; and
3. an image extracted from the quoted taxonomy/categorization (or relevant elements of it).

The list of the sources in order of appearance (from top right to bottom left) in the UNIDIR Taxonomy of ICT Incidents is as follows:

- Scott D. Applegate and Angelos Stavrou. 2013. "Toward a Cyber Conflict Taxonomy". 5th International Conference on Cyber Conflict (CYCON 2013), pp. 1–18.
- Chris Simmons, et al. 2009. "AVOIDIT: A Cyber Attack Taxonomy". Technical Report, University of Memphis, Number CS-09-003.
- 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.
- MITRE. 2015–2022. MITRE ATT&CK.
- Charles Harry and Nancy Gallagher. 2018. "Classifying Cyber Events". *Journal of Information Warfare*, vol. 17, no. 3, pp. 17–31.
- Ioannis Agrafiotis et al. 2016. "Cyber Harm: Concepts, Taxonomy and Measurement" (1 August 2016). Saïd Business School, WP 2016-23.

THE VECTOR

Scott D. Applegate and Angelos Stavrou. 2013. "Toward a Cyber Conflict Taxonomy". 5th International Conference on Cyber Conflict (CYCON 2013), pp. 1–18.



This work by Applegate and Stavrou was used to inform the analysis of the **Vector** cell of the UNIDIR Taxonomy of Malicious ICT incidents. In particular, their broad and inclusive classification of the vector was considered very suitable. At the same time, the full conceptualization of Applegate and Stavrou's taxonomy was not considered as it goes beyond the scope of the UNIDIR Taxonomy.

In Applegate and Stavrou's taxonomy, the authors outlined a categorization for cyber conflict events and the actors involved. The taxonomy has an interlinked data structure and can be extended. The overarching categorization concerns the differentiation between categories and subjects; the first one refers to the taxonomic classifications that are then applied to subjects. The latter are real-world entities such as individuals or other actors that feature in a specific cyber conflict event. Each of these macro-categories includes several sub-categorizations that cover more specific elements, and lateral linkages are used to describe the associative relationships between categories. Indeed, one of the purposes of this taxonomy is to link "actors with different methodologies, goals and patterns of behavior".[1] In their taxonomy, Applegate and Stavrou relied on pre-existing taxonomies, including AVOIDIT.

1 Scott D. Applegate and Angelos Stavrou. 2013. "Toward a Cyber Conflict Taxonomy". 5th International Conference on Cyber Conflict (CYCON 2013), pp. 1–18, p. 3.

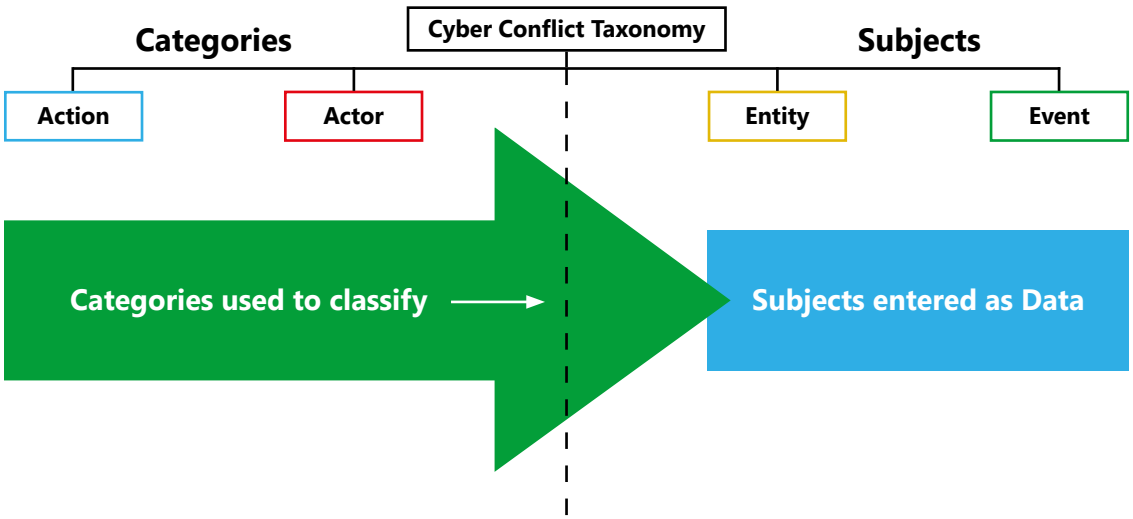
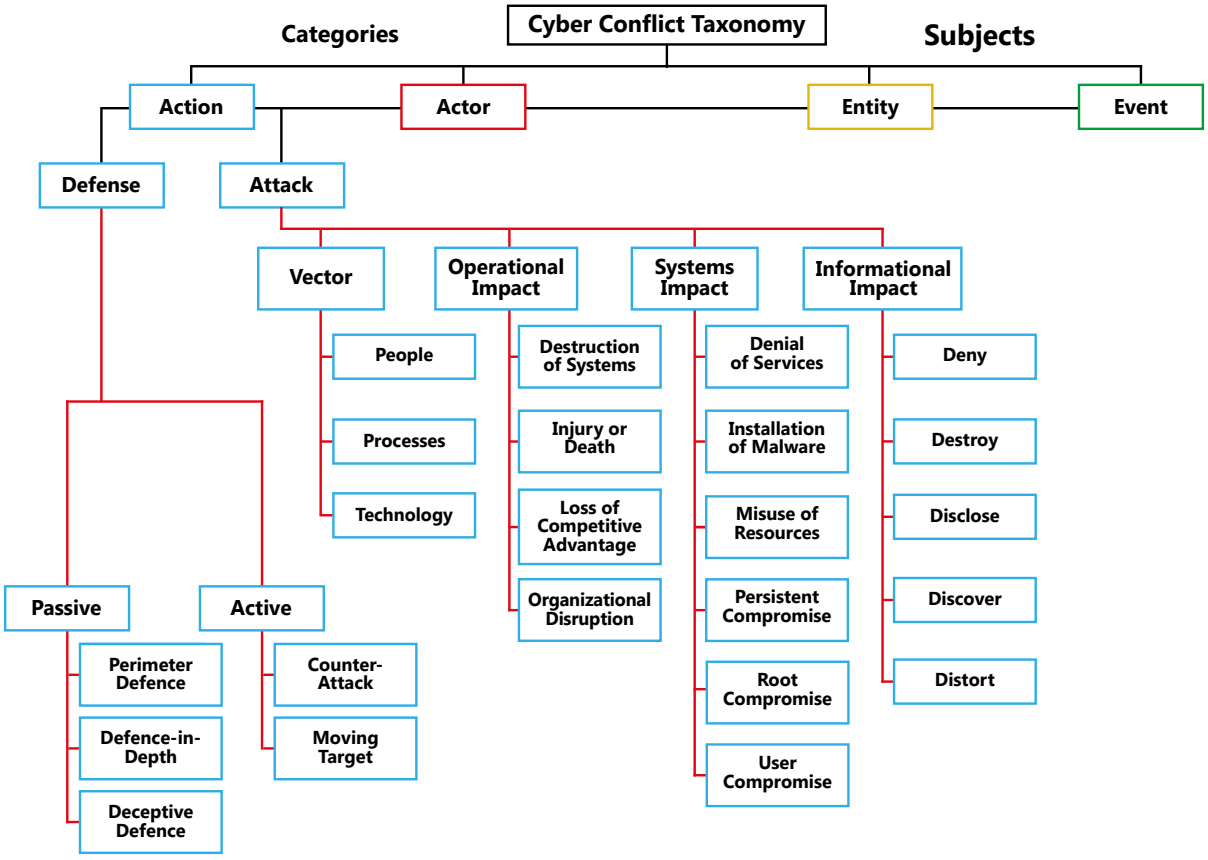


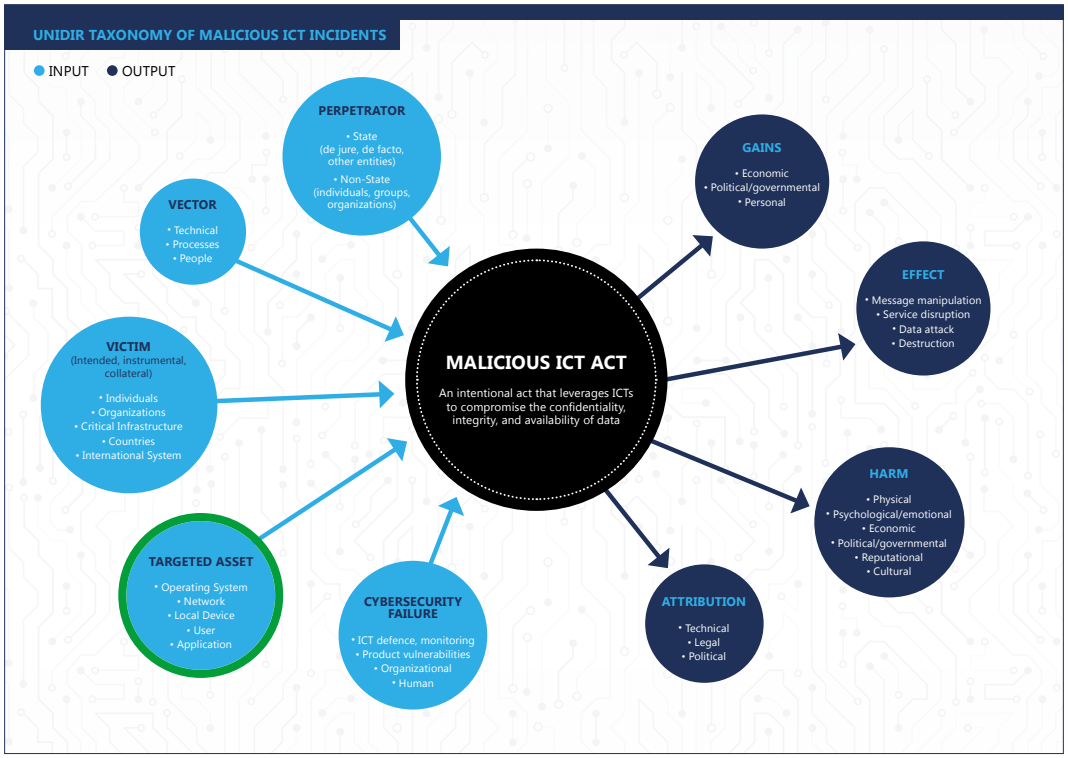
Figure 1:

Two segments of Applegate and Stavrou's taxonomy, "Cyber Conflict Taxonomy" (p. 6), and "Actions Category of Cyber Conflict Taxonomy" (p. 8).



THE TARGETED ASSET

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



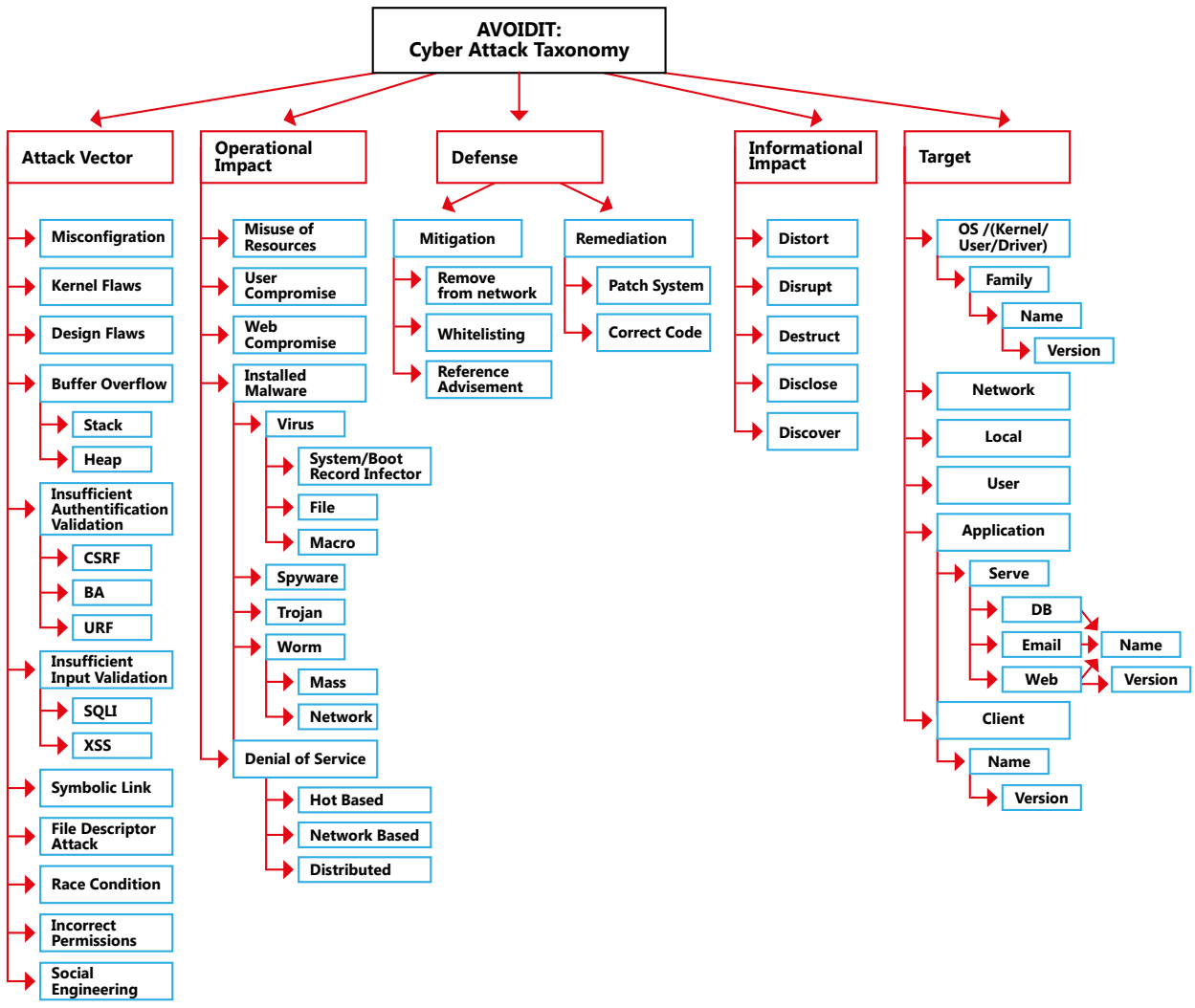
This taxonomy by Simmons et al. was used to inform the analysis of the **Targeted Asset** cell of the UNIDIR Taxonomy of Malicious ICT Incidents.

The purpose of the taxonomy by Simmons et al. is to identify and defend against the so-called cyber-attack. In particular, the authors propose a taxonomy that characterizes the attacks and the defence according to five major sub-categories: Attack Vector, Operational Impact, Defence, Information Impact, and Target (the initials of these sub-categories form the acronym AVOIDIT). According to the authors, AVOIDIT "provides … a knowledge repository used by a defender to classify vulnerabilities that an attacker can use".[2] Moreover, the AVOIDT taxonomy provides the defender with possible strategies to mitigate and remediate a malicious act. The authors affirm that AVOIDIT is useful for the classification of blended malicious acts, which are sophisticated acts that exploit multiple vulnerabilities.

2 Chris Simmons, et al. 2009. "AVOIDIT: A Cyber Attack Taxonomy." Technical Report, University of Memphis, Number CS-09-003, p. 2

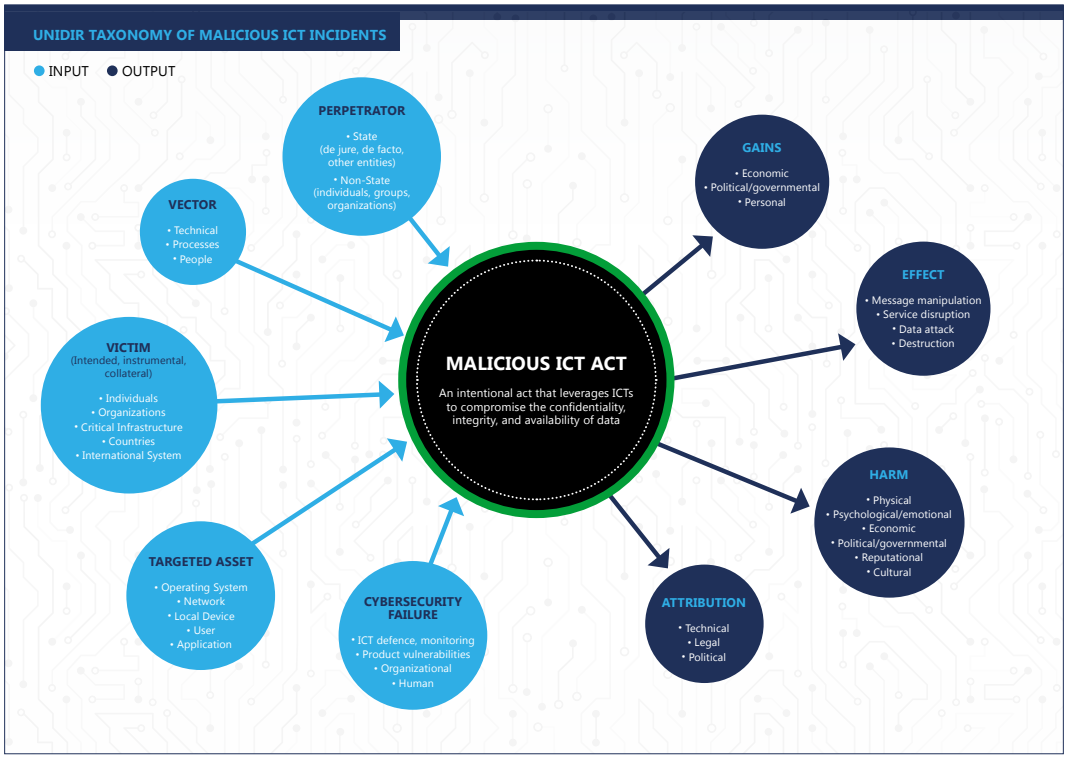
Figure 2:

The cyber attack taxonomy of Simmons et al. (p. 3).



THE MALICIOUS ICT ACT

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.



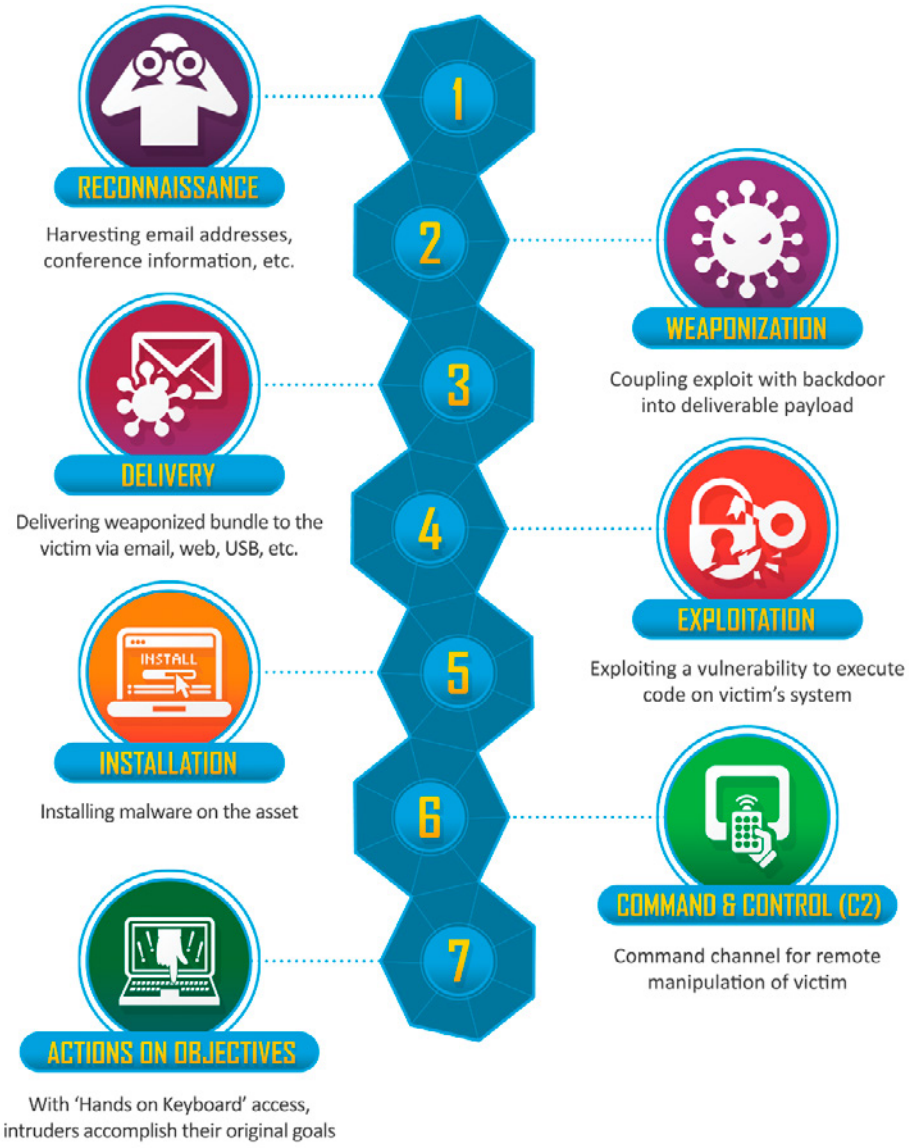
The UNIDIR Taxonomy of Malicious ICT Incidents does not provide a detailed analysis of the different steps of an ICT act. Yet, as indicated in the text, the Cyber Kill Chain can be used to further unpack and analyse the malicious act.

Lockheed Martin published this ground-breaking paper whose aim was to extend and adapt to the cyberspace domain the military concept of a kill chain, which is "a systematic process to target and engage an adversary to create desired effects".[3] The Cyber Kill Chain is particularly indicated to describe the so-called advanced persistent threats (APTs), and it outlines seven different phases of an ICT intrusion, from Reconnaissance to Actions on Objectives.

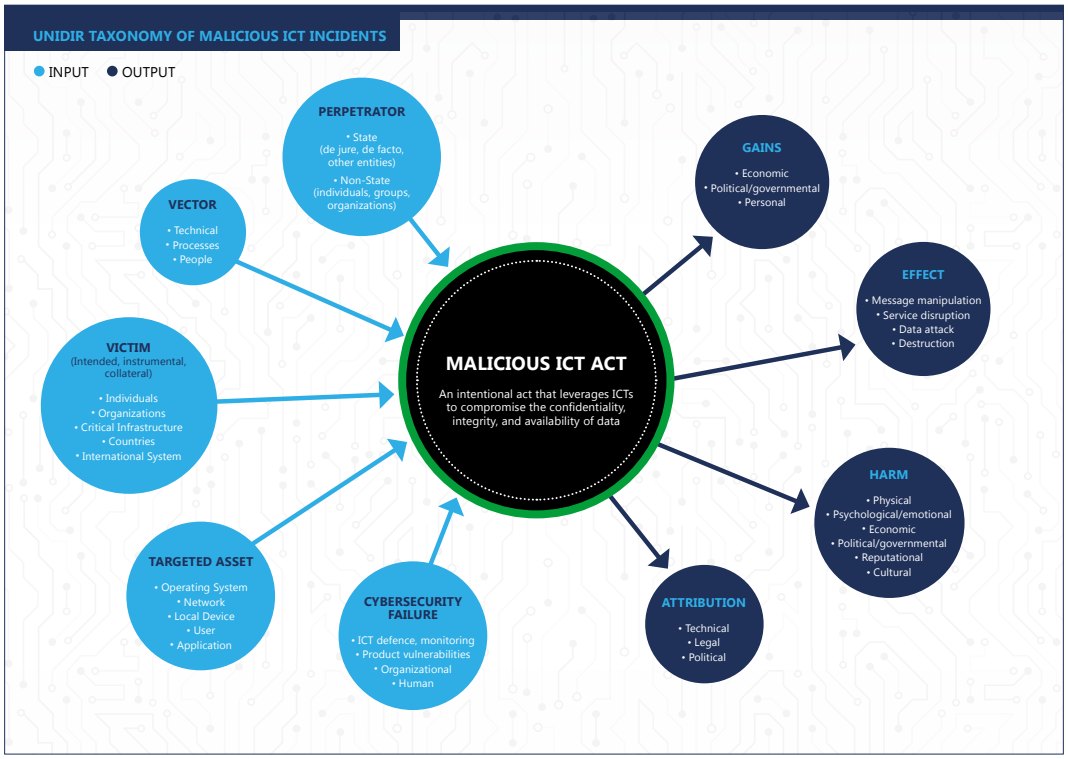
3 Eric M. Hutchins, Michael J. Cloppert, and Amin M. Rohan. 2011. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains". Lockheed Martin, p. 4.

Figure 3:

The Cyber Kill Chain from Lockheed Martin's website (https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html).



MITRE. 2015–2022. MITRE ATT&CK.

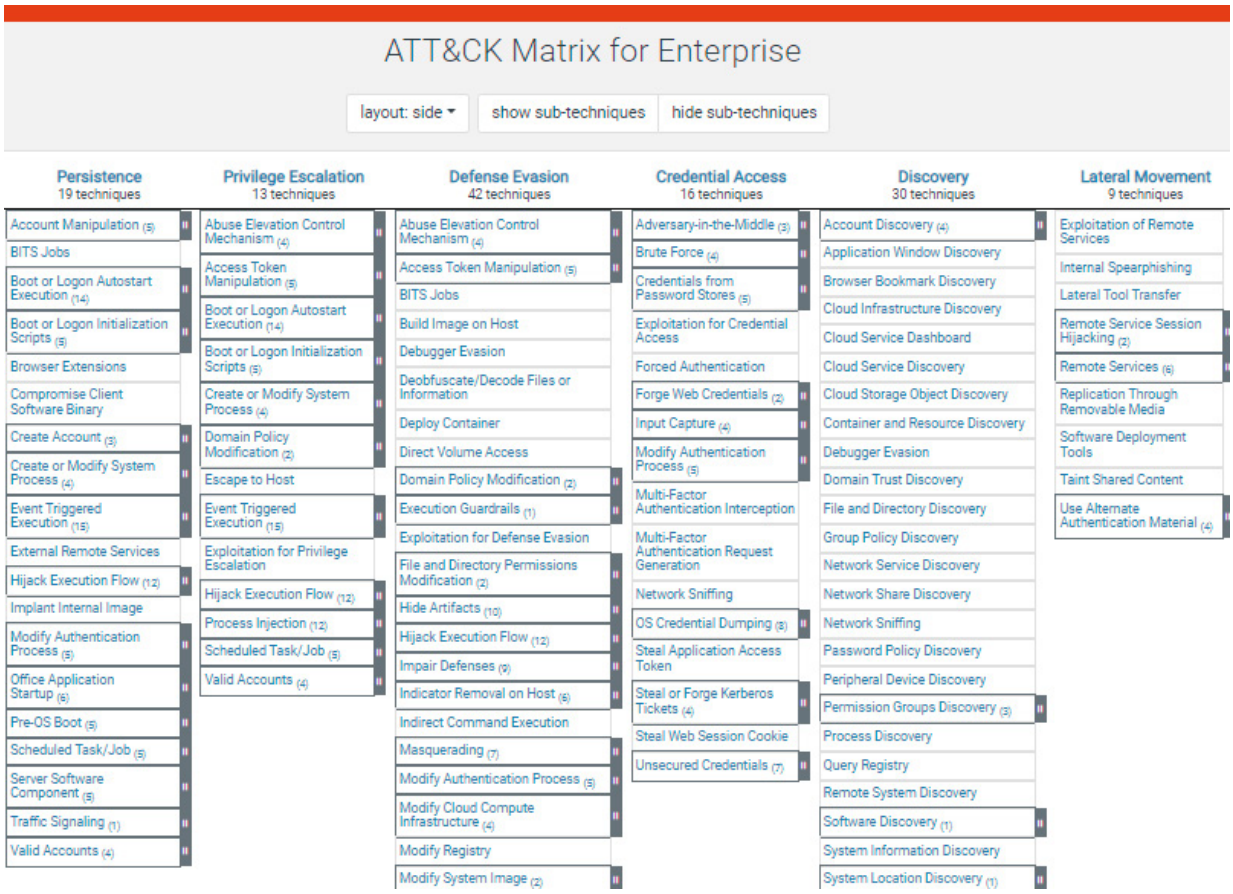


The UNIDIR Taxonomy of Malicious ICT Incidents does not provide a detailed analysis of tactics and techniques. Yet, as indicated in the text, the MITRE ATT&CK framework can be used to further unpack and analyse the **Malicious Act**.

The MITRE ATT&CK is not a taxonomy; rather it is a framework of adversary tactics and techniques based on real-world observations. As of August 2022, ATT&CK currently showcases three main matrices: Enterprise, Mobile, and Industrial Control System. Every matrix features a set of different tactics (from 12 to 14), labelled with the aim of the action performed (e.g., Reconnaissance, Lateral Movement, Exfiltration). Within each of the tactics, there are unique techniques, that represent 'how' the action can be conducted, and they are ordered alphabetically (e.g., Active Scanning, Exfiltration Over USB, Web Portal Capture), for a total of 335 techniques (the amount may increase over time).

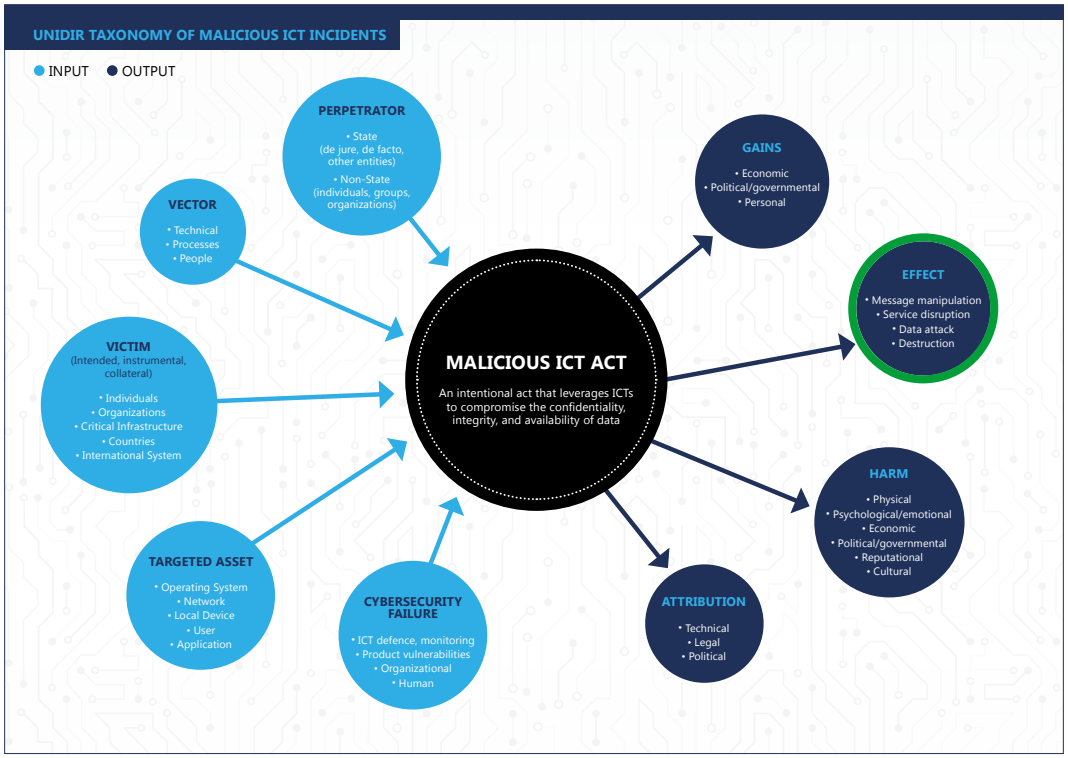
Figure 4:

An extract from the website of the ATT&CK Matrix for Enterprise.



THE EFFECT

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



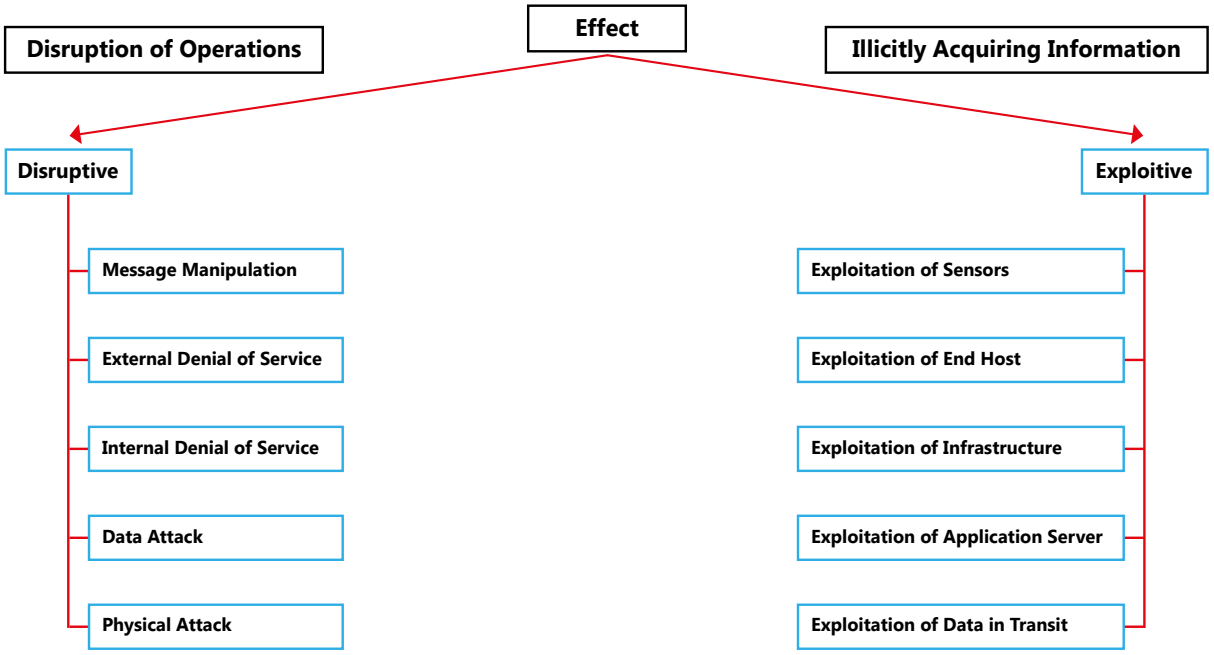
This work by Harry and Gallagher was used to inform the analysis of the **Effect** component of the UNIDIR Taxonomy of Malicious ICT Incidents. As explained in the infographic the UNIDIR Taxonomy only refers to disruptive effects, and it does not include exploitative effects.

Harry and Gallagher's taxonomy is oriented towards classifying ICT events focusing on the primary effects on a target. The authors' understanding of cyber events is particularly informative as they affirm that "cyber events are defined as the result of any single unauthorised effort or the culmination of many such technical actions that threat actors, through the use of computer technology and networks, use to create a desired primary effect on a target".[4] The authors classified primary effects into two main sub-categories: disruptive and exploitive. The former refers to effects generated by the disruption of operations (such as message manipulation, denial of services, and data attacks); the latter concerns the effects that result from incidents aimed at stealing information (such as exploitation of network infrastructure, or exploitation of data in transit).

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

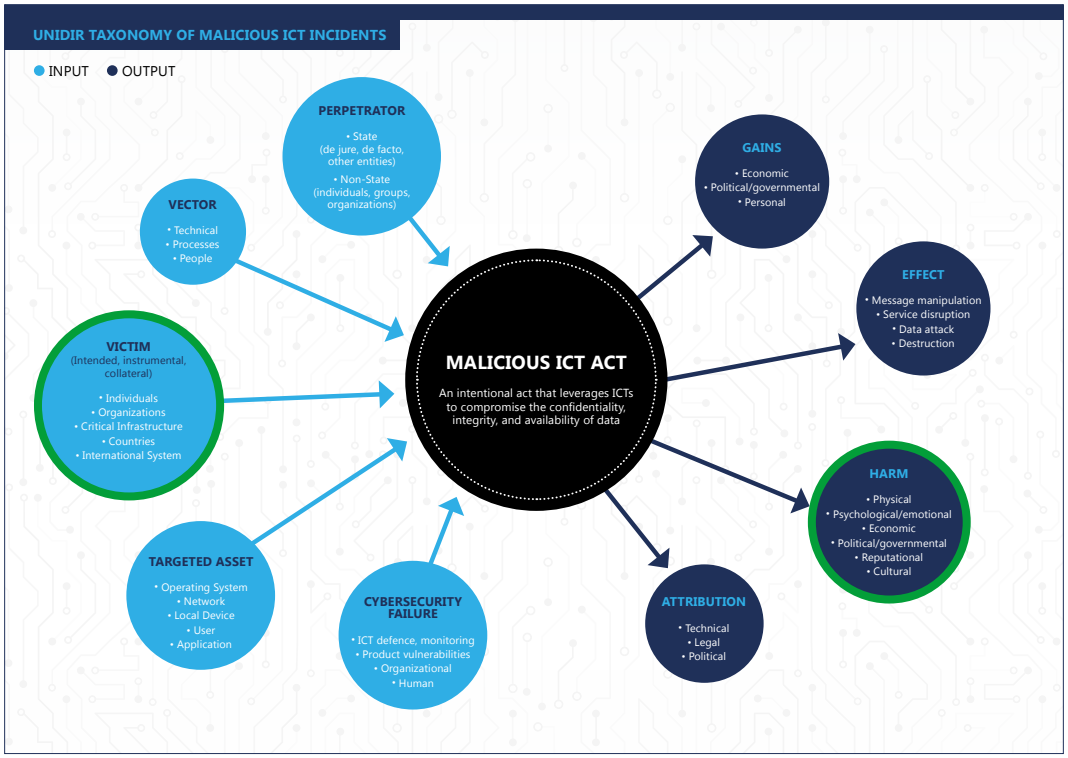
Figure 5:

Harry and Gallagher's "Cyber-event taxonomy" (p. 20).



THE HARM AND THE VICTIM

Ioannis Agrafiotis et al. 2016. "Cyber Harm: Concepts, Taxonomy and Measurement" (August 1, 2016). Saïd Business School WP 2016-23.



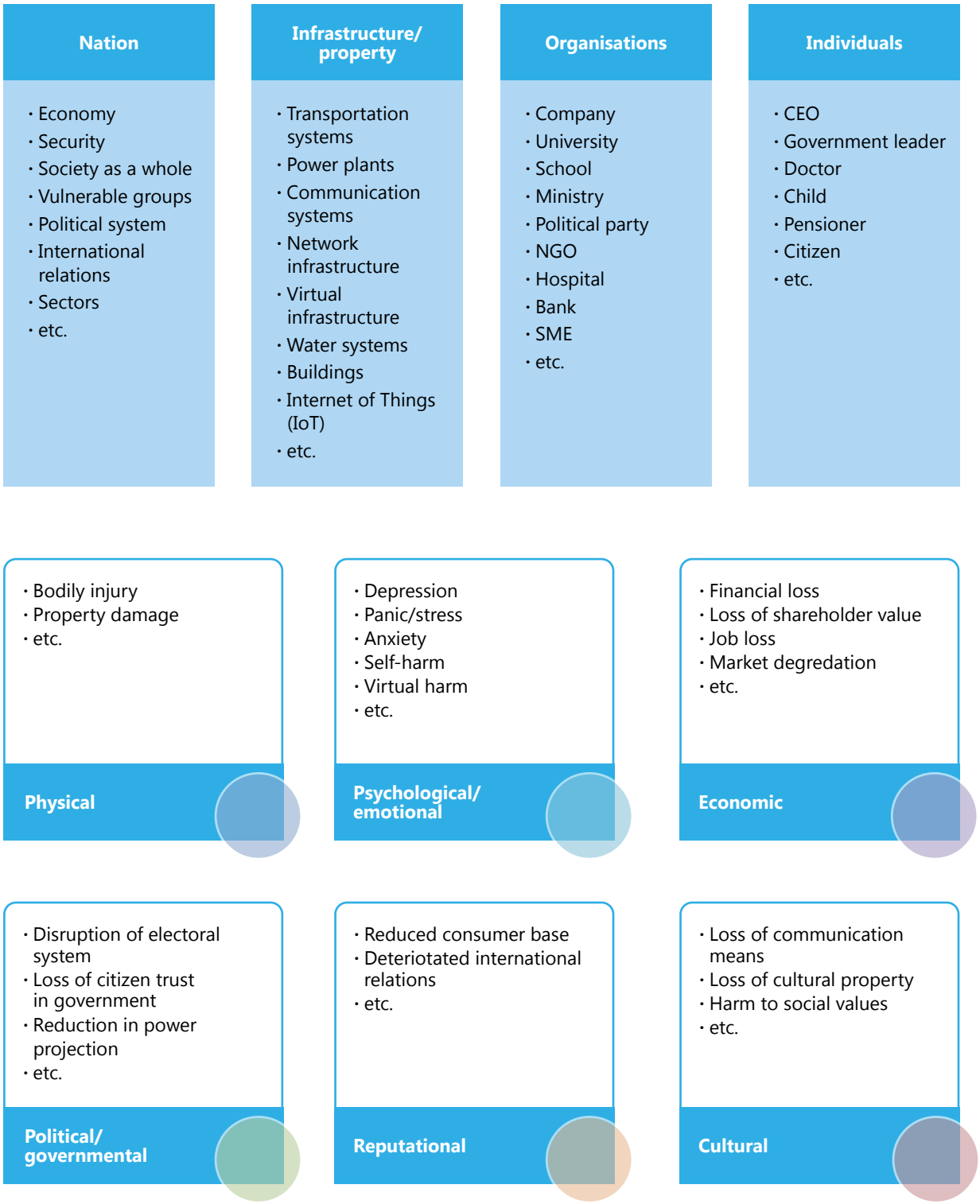
The UNIDIR Taxonomy of Malicious ICT Incidents referred to the work by Agrafiotis et al., mainly for what concerns the cell regarding the harm and for some of the items included in the cell about the victim.

The taxonomy of Agrafiotis et al. focuses on cyber harm, and it allows for a "better understanding of how harm is manifested within and outside of cyberspace".[5] It also sets an initial framework to assess cyber harm in national contexts. Cyber harm is understood as "the damaging consequences resulting from cyber-events, which can originate from malicious, accidental or natural phenomena, manifesting itself within or outside of the Internet".[6] The added value of this taxonomy is that it provides a more nuanced and adequate understanding of cyber harm than other taxonomies or classifications. On one side, it elucidates what are the subjects that may suffer from cyber-harm, and, on the other, it specifies different kinds of harm.

5 Ioannis Agrafiotis, et al. 2016. "Cyber Harm: Concepts, Taxonomy and Measurement" (August 1, 2016). Saïd Business School WP 2016-23, p. 1.
6 Ibid., p. 2.

Figure 6:

Two segments of Agrafiotis et al.'s Cyber Harm Taxonomy, "Examples of cyber harm subjects" (p. 29), and "Types and examples of cyber harm" (p. 30).




UNIDIR
UNITED NATIONS INSTITUTE
FOR DISARMAMENT RESEARCH