ROUTLEDGE FOCUS

# THE SOCIOLOGY OF CYBERSECURITY

## An Ethnography of a Science and the Profession

Marcin Zaród

ROUTLEDGE Focus

# The Sociology of Cybersecurity

This book explores the sociological processes related to digital infrastructures, nation-states, military organisations, companies and hackers. It explores how the European Union consults hackers, what the sociological implications beneath hacking tournaments might be, how the CVE system might be mapped onto the research of ICD-11 and how many theological devils fit as opponent models?

Based on ethnographic research conducted among hackers and cybersecurity conferences from several countries across Europe, *The Sociology of Cybersecurity* asks how knowledge is created in different groups connected with information security. It considers the ways in which social processes in the field of cybersecurity appear similar to phenomena that characterise knowledge production in scientific disciplines.

An examination of what the study of information security can contribute to our debates on privacy, digital economy, theories of sovereignty and critical perspectives in the 21st century, *The Sociology of Cybersecurity* will appeal to social scientists interested in the sociology of knowledge and contemporary research at the intersection of labour, technology and society.

**Marcin Zaród** is Assistant Professor in the Institute of Social Sciences at USWPS University, Warsaw, Poland. He researches the sociology of work, scientific knowledge and cybersecurity and is a member of Labor Tech Research Network.


Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

# The Sociology of Cybersecurity

## An Ethnography of a Science and the Profession

**Marcin Zaród**

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2026
by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
605 Third Avenue, New York, NY 10158

*Routledge is an imprint of the Taylor & Francis Group, an informa business*


SWPS University kindly provided funding for Open Access costs for this book through FRBN fund decision 47/2025/FRBN/D.



*British Library Cataloguing-in-Publication Data*
A catalogue record for this book is available from the British Library

ISBN: 978-1-032-50103-1 (hbk)
ISBN: 978-1-032-50104-8 (pbk)
ISBN: 978-1-003-39687-1 (ebk)

DOI: 10.4324/9781003396871

Typeset in Times New Roman
by Apex CoVantage, LLC

# Contents

SWPS University kindly provided funding for Open Access costs for this book through FRBN fund decision 47/2025/FRBN/D

Ethnographic and basic research for this book between the years 2014–2017 was funded by Polish National Science Center Preludium Research Grant 2014/13/N/HS6/04113 and visiting fellowship Etiuda Research Grant 2017/24/T/HS6/00081. Research on the profession between the years 2018–2021 was funded by Polish Ministry of Science Dialog Grant 0333/2018. The author has not received any funding from non-civilian, non-public or non-verifiable sources of funding.

# Introduction

How does computer security make knowledge? Is this knowledge a science? How have processes of formalisation of knowledge into science changed from 2013 to 2025? How is the shaping of this science interplayed with the changes in the profession and in the situations of workers, victims and clients? What institutions push for the science of cybersecurity? What is the politics of the science of cybersecurity? What is the relation between hacking culture and the politics of cybersecurity? If cybersecurity has some elements of practice that may be regarded scientific, then what are the equivalents of experiments, demarcation criteria, replication mechanisms and other philosophical and sociological issues known from studies in other disciplines? What is kept hidden from the public, and how can public understanding of cybersecurity be imagined? Finally, can or should cybersecurity become a science for the people?

Such questions may not have answers, and even if they did, this book may not provide them. However, this book would not have happened without an incessant curiosity that pulled me to those questions. While I situate my research as a sociological ethnography of the science and the profession of cybersecurity, the goal was not a vivid description of any particular community but a broad picture of the field at the scale that goes beyond any company, nation-state or cybersecurity specialisation. As with any model, the final result is both wrong and useful.

Wrong because it necessarily simplifies and reduces into the global pattern many subtypes that simultaneously exist while also neglecting some local counterexamples, resistance-practices and exemptions. This is why this book is wrong, as any generalisation has to be. Hopefully, it may also be useful because, by bringing together contexts from adjacent fields, thinking on wider scales may happen. After all, my work was also born because "someone was wrong on the Internetz".

This leads me to the ethical and epistemological paradox of this book. As a sociologist of science, I am doubly aware that natural, technical, biological and social sciences were active participants in the modernist, imperial project. The very ambition to propose a synthesis over what is otherwise a complex

DOI: 10.4324/9781003396871-1

and heterogeneous social reality of regions, groups that I have, at best, fragmentary understanding of, may be easily seen as a simple attempt to continue this project. Being aware of this risk, I propose my answers to the questions stated before as sociological concepts relevant on the global scale, at least for English-speaking or NATO-influenced countries.

As a sociologist, I have but one answer. Work. Work is neither the only political component of cybersecurity, nor is wage labour the only form of work, but without factoring in the issue of work or labour, I firmly believe that any understanding of cybersecurity is incomplete. Consider three cases. Firstly, a cybersecurity study of the evolution of attacks on the infrastructure of hospitals in Ukraine and Europe after 2017. Secondly, the evolution of privacy for activists, medics and maintainers of infrastructure who work in Palestine, Eritrea or Kashmir. Thirdly, the development of automated, artificial intelligence–based systems that try to appraise the companies that develop cybersecurity products against the groups in the previously mentioned two cases.

If there is one conclusion of my book, it is this: only by recognising work that goes in cybersecurity, which, in turn, goes for and against enabling, maintaining, enclosing or destroying knowledge that goes with work of other people, can one even begin thinking about science, knowledge, power or work in any social science in the digital era.

The book's title came as a result of this understanding. The ethnography is a method, but not the goal. The science of cybersecurity was and still is "in the making", instead of something made and demarcated. Cybersecurity science is easier to understand through negotiations over systematics, generalisations, comparisons and interpolations. However, those processes of systematisation, institutionalisation and underwriting of risks go together with processes of professionalisation, certification and appropriation of unpaid labour. The nebulous, hidden and mosaic character of cybersecurity science is in dialectical interplay with more and more overt dimensions of the profession. Hence the title: "a" science, but "the" profession.

This is why my understanding of cybersecurity as a science and as a profession is heavily influenced by the Marxist tradition and its recent resurgence. Johan Söderberg and Maxigas (2022) have shown how companies capture free labour without paying for it, illustrating how hacking's commitment to autonomous infrastructures turns the critique of digital capitalism into a mechanism of accumulation. Söderberg and Maxigas have shown dialectics of hacking while also showing that the concept of the "Californian Ideology", as described by Richard Barbrook and Andy Cameron in 1996, is still relevant. Matteo Pasquinelli (2023) not only theorised and evidenced algorithmics embedded in surveillance, imitation and violence on the workers and citizens but also has shown how algorithms gatekeep and extract the knowledge that circulates in social groups.

It would be misleading and scientifically dishonest not to mention the immense contribution of anti-colonial, black and feminist studies of

computing, labour, feminist scholarship and others. Among them, I relied on Caitlin Rosenthal's (2019) original research and Meredith Whittaker's (2023) summary on the origins of Charles Babbage's architecture that came from the plantations of the East India Company. Similarly, I took much both from hacking studies by Biella Coleman (2013) and from feminist studies of cybersecurity by Christina Dunbar-Hester (2019) and Amanda Levendowski (2022) as well as cybersecurity post-colonial studies in international relations by Anwar Mhajne and Alexis Henshaw (2025).

Chapter 1 starts with vignettes of work. Hackerspaces in Eastern Europe from 2010 were not the only places for invoking hacking culture or for gathering new sub-strata of IT contractors, but they were also the frontiers of gentrification and communities that functioned as communal cybersecurity laboratories. It shows how labour, social mechanisms of cybersecurity learning and hybridisation of the work of administrators and developers established the background of the seismic shift of General Data Protection Regulation (GDPR) in the European Union. Chapter 1 serves as introduction to my method and some theoretical concepts as well as examples of interplay between everyday maintenance and the glamour of cybersecurity. While I did not have enough space to discuss it at length, significant parts of this chapter were built in discussions with Winnifred Poster (2026) and the Labour Tech community. This allowed me to partially validate many findings beyond the context of Europe, for example, for IT subcontractors from India or Brazil.

Chapter 2 builds on the previous one, as it describes the sociological model of the cybersecurity laboratory and the concept of a thought collective, modifying the term coined by Ludwik Fleck. A laboratory is the workplace, and a thought collective is the intellectual milieu. Between them, knowledge and/or science happen. The basic sociological premise of Chapter 2 is simple: the cybersecurity laboratory is the sociological group-space that has the power to abstract, to create what I will later define as "stabilised instabilities". While all scientific laboratories in general do this, cybersecurity laboratories do this on the digital infrastructure, so, in a way, they are nested one layer of abstraction further. This is why cybersecurity laboratories are second-order laboratories: they are laboratories of laboratories, as they make abstractions, rules and "stabilised instabilities", functioning with things that other laboratories and, broadly speaking, digital infrastructures in general made replicable, stable or reliable, at least as a rule of thumb.

As a particular example in Chapter 3, I describe how playing Capture the Flag (CTF) tournaments is a constitutive labour for thought collectives, serving as a mechanism for social inclusion, prestige and knowledge replication. Such social mechanisms not only are captured, in ways similar to those described by Barbrook and Cameron, but also held as useful institutional interspaces that catalyse exchanges and reduce costs of training. Thus, Chapter 3 is the study of recuperation, or the recapture of critique and culture for making it into unpaid labour. As far as I know, this is the first ethnography of science in CTF that has been published to date.

If Chapter 3 shows cybersecurity cognition in the wild, or in an informal setting, then Chapter 4 focuses on the epistemology of cybersecurity as a science. I start with theorising "stabilised instability" in order to discuss cybersecurity systematics, such as Common Vulnerabilities and Exposures (CVE), and their application in the military, insurance and research fields. I also outline a premise for a different cybersecurity science that I call "cybersecurity for the people". As far as I know, this is the first attempt to theorise cybersecurity systematics as connected with nation-state interests, epistemology and labour.

In Chapter 5, I investigate exclusion from cybersecurity education, and I add theorisation on the issue of queer hacktivism and its potential capture by nation-states. Finally, I note the potential of feminist cyberlaw and its connections to modern, progressive, universal and scientific cybersecurity for the people.

I do not believe that I have found the satisfactory answers for questions I have asked in the beginning. I believe, though, that I asked those questions in an interesting way. If there is one theoretical conclusion that I wish to offer, then it may be this one: both cybersecurity and sociology are inherently interested in the delicate balance of the norm and the exceptions, as well as their justifications, protections and the precious value of both exceptions and standards.

As far as I can understand, key contributions of this book include: (1) the theorisation of cybersecurity laboratories as second-order laboratories; (2) conducting and interpreting the ethnographic study of Capture the Flag tournaments as replication of cybersecurity knowledge; (3) conceptualisation and examples of discovery in cybersecurity, understood both as epistemic and a social mechanism, which provides a baseline for public understanding of cybersecurity; (4) recognising that after 2020, critical computing and AI studies have to include theorisation on cybersecurity and its systematics; and (5) connecting cybersecurity systematics with theorising on the philosophy of cybersecurity, sociology of hacking, studies of Capture the Flag and debates on digital infrastructures.

After all this labour, I still study cybersecurity with a mixture of curiosity, hope, fear and disgust, not dissimilar to the approach I have to sociology and science in general. To paraphrase what Zygmunt Bauman wrote to sociologists (1988): for better or worse, sharing the ideals of modernity as in all academic fields, cybersecurity for the people should aim for reason-led improvement of the human condition. It should aim to increase the volume of human autonomy but not the kind of autonomy that, in absence of solidarity, results in loneliness. Conversely, to increase the volume of human solidarity, but not the kind of solidarity that, in absence of autonomy, results in oppression. It should also show how humans, governments and organisations create digital infrastructures, making humans more aware, rational and involved in decision-making concerning infrastructures. Similarly, cybersecurity for the

people must show communities how large groups can maintain and develop digital infrastructures to organise new forms of common knowledge, communications, ecology, care, joy, love, privacy, trust and various other dimensions of human life.

I am immensely grateful for the time and effort that my colleagues devoted to this ethnography. The interviewees who kindly agreed to be observed or people who agreed to note their words in an anonymised version are my colleagues, not because I compare to them in cybersecurity knowledge but because every human is an intellectual (Gramsci, 2007). Without a doubt, many of them would not agree with the interpretations given in this book, but I am more than certain that for at least a moment, they shared at least the curiosity.

## Fieldwork. Data. Limitations.

As any hacker or engineer will tell you, tools should not be blindly used but understood. Social research is no different, so, when making comparisons, I will do so symmetrically in two moves. I will constantly examine similarities between practices well understood by sociologists of science and practices I saw as a sociologist among security researchers and hackers. However, recognising similarities, while useful, may lead to cognitive biases. So, in every ethnographic vignette, I will also try to recognise differences – not only in terms of money, prestige or the public visibility of failures but, more importantly, those involving understandings and social dynamics around experiments, computer vulnerabilities or designed infrastructures.

As I mentioned, the project is influenced by various notions of dialectics. In practice, that means that I am always looking for ways to contradict my previous viewpoints or to extend the perspective into a different scale, to see what was the norm as an exception, and so on. As a result, the book may appear as slightly abstract and self-contradictory. Since this book developed from my first academic project, for most of the time, I had no access to cross-coding validation. Instead, I opted for a "do-it-yourself" version of community validation or participatory action research, which means that I asked the ethnography participants whether they agree with my reasoning and interpretation. If not, I noted discrepancies and will report them accordingly in my book.

I staunchly believe in paying participants for their co-validation because I believe that I should be paid for ethnographic work, so as a logical consequence, they should be remunerated also. Contrary to my ethical principles, in most cases, the rules of my funding providers did not allow it. Nevertheless, I asked the majority of participants about remuneration, openly stating how my finances were at the moment. A majority of them declined, mostly because cybersecurity work pays much more than social sciences. In some cases, we came to a mutual agreement that I could contribute their remuneration to a

social cause, like science education, sponsoring tickets for conferences or small support for a local coding-inclusivity event.

All ethnographic observations were made with full, repeated and informed consent of individual members. Exceptions were made for large public events like conferences, where such consent was not practical for logistical reasons. In such cases, I did not make pictures nor record names. In selected cases, some security researchers asked for erasure even from such record, so I abstained from transcribing the observations from the physical field notebook to a digital version, and I destroyed the physical page.

The core research for this book is based on a series of studies I conducted from 2014 to 2020 in various countries in Central and Western Europe. I spent 150 days observing informal hacking communities in the region. Additionally, I participated in security conferences, and I observed Discord chats on cybersecurity research, such as the FHE.org community. Since Discord and chat inquiries were supplemental, I recorded them only when I had the consent of the community and all people on the recorded fragments.

To extend the perspective beyond Europe, I interviewed 30 security researchers (security architects, cryptographers, ex-CERT members, etc.) from five countries. In addition, I visited five computer security conferences and two academic computer security laboratories. I also observed in real time how hackers, academic researchers and security specialists interacted during the Chaos Communication Congress (C3) from 2015 to 2019 on selected workshops under conditions of anonymity. I also observed workshops on security conferences other than C3, under the same conditions of consent, but I wish to keep the conferences anonymous. I deliberately had not asked about matters that may breach confidentiality agreements.

A dialectical approach and interests in synthesis and in personal accounts resulted in a technique I called "field-contrast expert technique", which boils down to approaching the interviewee as an expert both in the field and in the subjective interpretation of it. This technique of semi-structured interviewing follows questions such as, "what explanations about this big vulnerability/hard question from 1–2 years ago did you discover" juxtaposed with contrasts like "on what elements of this thinking of your peers you do not necessarily agree?". As a result, the interviewee was able both to generalise about "what is commonly understood", or the good ol' sociological cliché, "what does your [imagined] colleague say about it?", and to highlight issues in which they personally differ. Adding this kind of hypothetical clauses or projection techniques, as well as asking about vulnerabilities that fell out of their current workplaces, allowed people to speak somewhat more freely, without increasing the risk of breaching their non-disclosure agreements. If they used too many details, I erased the recording. Through the whole project, I used an older type of audio recorder, without an Internet connection.

I spoke off-the-record with military computer security recruiters, policymakers and some people from what seemed to be intelligence agencies. This

is not an unfounded suspicion, as two times I have been asked to join the intelligence services, an event not usually recorded in ethnography, except for CIA assets like James C. Scott or colonial ethnographers.

In addition to individual interviews in the field, I recorded over 150 samples of "fresh talk" – the kind of talk between professionals which occurs when they try to solve a complex issue. To sum up, the database for this research has 300 records and about 2,000 cross-analysed fragments. Material was reviewed and updated between 2023 and 2025 by additional desk research, follow-up interviews and participation in cybersecurity conferences.

All the participants were informed about my research interest and the moments I started to "make ethnographic observations", that is, when I turned on the recorder. All the participants who provided data to the database did so with informed and repeated consent and with information on where they could make a professional complaint to my research institutions. I asked for consent after recordings and gave access to individual data to people participating in the event for verification purposes, with access to others' data restricted.

Between 2013 and 2020, I conducted five workshops in the communities I worked with, showing my approach to analysis and my claims. I also prepared workshops and lectures for the biggest hacking convention in Europe (Chaos Communication Congress) and showed my data at security events in the region (Oh My Hack, Confidence and some conferences of Institute of Electrical and Electronics Engineers – IEEE, Association for Computing Machinery – ACM). While I interviewed researchers from United States of America, I did not conduct extensive ethnographic research there. When it was politically viable, I had not enough funding. In the middle of 2025, politics changed, but insufficient funding remained an issue.

Where events are quoted or described in detail, the participants gave sustained consent and had an opportunity to access raw data on them and to inspect my anonymisation routines in my previous publications (Zaród, 2016, 2018, 2022; Kostyszak et al., 2015). If some examples described in the book lack technical data, it is to preserve the anonymity of participants in a small field. The only person responsible for technological inaccuracies is the author, as sometimes data was inaudible or inscrutable without putting participants at greater risk.

This research protocol was based on what I consider "best standards" of ethics in sociology, as described in ethical procedures from Polish, British, US and international sociological organisations (PTS, BSA, ASA, ESA, ISA), deliberately choosing to gather less ethnographical data and to opt for maintaining more privacy for the interviewees.

With the ethical and methodological choices I made, I had far less access to organised laboratories than my colleagues researching other disciplines. Quantitative studies of the field are challenging since the publication structure is based much more on a nebula of Twitter posts, conferences, press releases and informal channels than on journal papers. The equivalents of Nobel

Prizes are harder to point out and are not as widely recognised. Making matters worse, it is widely assumed that military intelligence agencies are large institutional nodes, in terms of sheer recruitment, research and sponsorship. I focused on this topic in Chapter 4, but it is only the tip of the iceberg.

This book, while often critical of cybersecurity science developed in the service of the military or institutions of surveillance capitalism, is as much a critique as it is a sociological attempt to propose some tools to interviewees and other cybersecurity researchers that perhaps may be useful for shaping their professional and scientific field. In this sense, this book is written between traditions of John Bernal, Lila Abu-Lughod, Olga Amsterdamska, Joseph Needham, Hilary Koprowski, Ludwik Fleck, Antonina Kłoskowska, Nadera Shalhoub-Kevorkian and many other scholars. Cybersecurity should become science for the people, science done by the people and science accountable to the people. This book aims to contribute to this goal. The definition of "people" is not limited to "cybersecurity researchers" or "citizens of the Global North", for details, read Bernal.

This is also why I deliberately refuse self-colonisation. This is not a book about "cute exotic case-study cybersecurity from Central-Eastern Europe"; although, for many English-native researchers, such a book would be much easier to grasp and, perhaps, much more citable. No, cybersecurity is a global field, so I will research it as so. If Poles, Americans, Ukrainians, Germans, Swedes, Romanians, Czechs, Koreans, Brazilians or Palestinians of all genders and fur colours,[1] work as subcontractors for American oligopolies, I will interview the labourers and work it out from the bottom as sociology of work always has. Cybersecurity subcontractors may be labour aristocracy in their respective countries, but for oligopolies, they are a dime a dozen, replaceable when they suffer burnout or when nation-state politics change.

Also, to make myself absolutely clear, there were more than enough researchers or hackers from the Global North who gave me interviews or helped by explaining standards. There were more than enough researchers who helped me, not out of frustration, but out of honesty. A majority of them would not agree with my left-leaning perspective, but they shared my sympathy to dive deep and talk openly about it.

I am thankful for the time and labour of people who agreed to be observed and to give interviews or unrecorded talk. I am grateful to people who provided consultations and spent time to agree on disagreements with me. Ultimately, I take responsibility for this book and this research.

## Note

1 Hacktivism and cybersecurity normalised "fursonas", welcoming and normalising online identities of various "furry" groups and humans. This will become theoretically relevant in Chapter 6 for discussion of subversive practices.

# 1 “Kaleidoscope.”

## Maintenance. Infrastructures. Abstractions.

To understand processes at the scale of the field, I would like to start with its margins. To understand what happens behind the confidence of non-disclosure agreements on the global scale, this chapter investigates communities of programming and computer administration subcontractors in Europe.

The methodological trick here may be as old as labour research. If workplaces are barred by non-disclosure agreements, go look for social spaces where groups interact after work. Do they have social clubs, DIY groups, conferences, prizes and other prestige events? As I was absolutely honest about my goals, the majority of interviewees immediately recognised that the difference between sociology and social attacks in cybersecurity lie in justification, ethics and social legitimation but not in method. Like a red team (the attacking side) investigating the weakness of a social system, I looked for subcontractors. As the field is rich in multi-faceted irony, cybersecurity researchers referred to my academic peers not as “professors” but as “generals”.

Generals, field report. There is only techno. For newcomers, it might sound like Slavic folk-themed, gopnik, techno, hard-bass whatever. For connoisseurs, it is immediately recognisable as a classic remix of a musical theme from an old computer game, Tetris.[1] If you hear obnoxious Slavic beats around heaps of electronics, you tune in to Central Europe no matter whether you’re in Poland, Czechia, Lithuania, Ukraine, Russia, Shanghai, San Francisco or Gaza. It’s not meant to be pleasant – it’s meant to be mind-burning and gradually exhausting, bringing death by a thousand cuts for those who do not share the same foibles.

The purpose of obnoxious beats is the same as the purpose of archaic conference posters, stacks of books or whiteboards full of equations in laboratories: to demarcate. Not only to socially exclude but to demarcate as it is understood in philosophy of science, that is, to establish a separate, safe mind-space for those who are included in the field. To lower the cost of cognitive failure by proximity of the trade and to help to maintain the focus.

What is the relation between the vibes described in the previous paragraph and the goals of this book? First, in places like those described, one can meet cybersecurity freelancers that work in security teams of various digital

DOI: 10.4324/9781003396871-2

corporations. While freelancers often "grow up" out of their hackerspace, they often hop in when they visit the city or when they look collaborators for either complex or private projects. The mechanism here is very similar to the "homel lab", the group when one does their master's or PhD thesis. One may move out of it, specialise into a different field or fall into a conflict, but those are the nodes of the network.

The key methodological issue was patience. Instead of asking about vulnerabilities, scandals and illegal stuff, I was able to learn much more when I took an interest in reverse engineering or figuring out how things work from having physical access to the object, in areas such as obsolete computing systems or old telecommunication equipment.

Only after gaining trust was I invited to more closed-door meetings and conferences. Eventually, as I helped with my knowledge as a sociologist, science communicator and organiser, I was invited to a workshop on the European Union's General Data Protection Regulation.

Those are two arguments for the relation between informal groups and the cybersecurity as a whole. Firstly, informal groups serve as places of education and "maternal labs" for experts and freelancers. Secondly, through my ethnographic work among informal groups, I was invited to a closed-door consultation workshop by an aide of the European Parliament (EP). Hence, the relation: informal groups facilitated expertise that was recognised by the transnational political institution of the region I conducted my study in. An EP aide was conducting unofficial consultations for what later turned out to be one of the resolutions within the General Data Protection Regulation (GDPR), an EU act that made a significant change in digital markets, including cybersecurity.[2]

But, before discussing global affairs, I wish to show how hackerspace enables experiments in a smaller scale. To understand Fragment 1.1, some context may help. As I said, we are in a place with numbing techno audio. It is in a basement. There are not many people nor much light here. I navigate it because I'm familiar with the space. I have been doing ethnography here for several months. I am getting around the place, but I still had not found out the relation described above. There is a table, two people and a bottle of beer. I recognise the people as Speck and Fidel, and the beer is a bitter from wheat and barley malt. The beer and the vibes are similar: everything is light and casual with just a drop of regional spleen. I won't drink today, but on another evening, I might have joined them. I won't take notes or make an effort to remember anything on this occasion. The evening is young in our hackerspace.

I place myself closer to Speck. Both hackers have already openly consented to participate in the research, under the condition of anonymisation of company, city and nickname. They will have access to source material for this book in the local repository for the community I am writing about.

Fidel is younger, just finishing a high school programme for the mathematically gifted and working part-time for a company. He is into cryptocurrencies, the free market and misogyny. Speck is older and works full-time in

system operations (SysOps). Fidel is stronger in theory and network science. Speck has more practice in maintenance and error-handling. Fidel is skinny, while Speck is bulky but still welcoming.

The company they both work for is understaffed. Their "urgent/critical to-do list" (backlog) gets longer every day. Speck is slowly getting frustrated, as he sees that more of his colleagues from abroad pursue careers in development operations (DevOps): less concerned with maintenance and more with development. DevOps means better pay, more prestige and more engaging tasks.

They sit on a sofa, split between an evening chill-out and a discussion of a server load balancing experiment. It will use infrastructure that belongs to the hacking community in order to test a hypothesis they are curious about. This is not unusual practice, so the community maintains a couple of servers and services with backups, usually accessible for such work.

The experiment cannot be conducted on critical (or "live") infrastructure, such as a membership or fee collection system, but spare servers should be made available to them. Both Speck and Fidel are regular members of the "space" (abbreviation for hackerspace), so neither of them expects any objections. The final decision about the experiment would be made by the server supervisor (nickname: Rama) or through community consent during one of the regular weekly meetings.

The results of this experiment are not exactly vital for the professional lives of either of them. It is more a matter of professional curiosity or ambition to "go beyond being a mindless fucking subcontractor for the Yanks" (translated *in vivo* quotation from the talk). Their company refused to give them resources, so they experiment in their spare time. In short: servers in this hacking community are test beds because engineers have found that it's easier to set up experiments here than to handle the official procedure in companies. As far as I know, no internal company data is to be used, only artificial equivalents necessary to simulate appropriate conditions (e.g., fake email traffic, fake database queries, fake database data consisting of chaff instead of valuable information).

The hackerspace has some spare servers. They aren't quite high-tech, but they are good enough for test purposes. The community acquired them when the local telecommunications company was modernising. As the space has some renown in the country, people from the telecom passed through and asked if the space wanted some stuff. So, the stuff landed in the basement, ready to be used by Speck and Fidel (see Fragment 1.1 for a quote from a DevOps from the hackerspace).

## Why Do SysOps Matter?

I will return to the rest of the hackerspace evening in a moment, but I have to pause here to put some focus on the infrastructure. This is something that is easy for a layperson to neglect. As the old adage says: "newcomers talk

> Hackerspace infrastructure is rather safe and fail-proof. There is a separate backup for critical services, like mail, webpage and so on. It has to be always available; we do not mess with it. Everything can be modified or experimented. For example, right now Wi-Fi is down because Hammurabi was playing. Deal with it. So, it's a rather safe place, of course, if you use firewall and VPNs, but at the same time, Hammurabi and others have many ideas about what else could be modified or upgraded. You could just sit along and see how it's done. So, in effect, there is a lot of stuff that is being introduced, because someone had such a mood. But in the end, you see a lot and learn a lot, which helped me a lot.

*Fragment 1.1* This is a spontaneous demonstration given by hacker. It examines aspects of hackerspace infrastructure. I noticed that hackerspace infrastructure is in constant refurbishment and negotiation. For hackers, this is a positive trait, as it provides learning opportunities. This is an excerpt that demonstrates an initial phase from a longer, repeated pattern of collaboration, not a singular example.

strategy, experts talk logistics". In this case, strategy means offensive or defensive hacking. Logistics means everyday handling of infrastructure.

This adage could be applied to "Science-Technology-Society" (STS)[3] ethnographies of laboratories and to non-STS studies of hackers as well. Earlier works focused on communities of high renown: the place where the polio vaccine was researched (Latour & Woolgar, 1986), the world of high-energy physics (Knorr-Cetina, 1999), NASA Rover missions (Vertesi, 2015), the Anonymous collective (Coleman, 2015). I enjoyed these works, and my own work would be impossible without them.

My strategy for understanding the transformation of hacking knowledge into the science of computer security is different. My concept of computer security relies on treating it as both infrastructure (Bowker & Star, 2008; Star, 1999; Star & Ruhleder, 1996) and a mechanism similar to scientific facts (Fleck, 2008). This may sound overly complicated and over-theorised, but it is just a way of saying that I need to constantly understand the connection between SysOps in the subsidiary of the Big Bank in Poland, the Big IT Mogul and the theoretical cryptographer at the Big University. Practically, it means that I will have to move between concepts from studies of technology and studies of science. While they are often taken together, their nuances will soon become important.

To benefit from some of these nuances, I will use the concept of infrastructure as understood by Susan Star and her co-authors (Bowker & Star, 2008; Star, 1999; Star & Ruhleder, 1996). They noted several socio-material traits of infrastructure that I took special interest in during my fieldwork, and I wish to develop these conceptually through the book.

Instead of explaining them, please do the experiment with interpretation of qualitative data yourself. Go back to Fragment 1.1 and look for traits of infrastructure as predicted by Star and others. Infrastructure will be hard to observe until it breaks down; it will grow in small increments and only rarely in big sweeps, and it will be learned as part of membership in a community. It is embodied in standards and in the bodies of users and operators. It is also embedded in myriad other social agreements and technologies. It is always highly localised, yet it always goes beyond a single location.

One thing is to note that hackerspaces work on their own infrastructures, in a manner resembling fractals, the ouroboros or any social group deeply vested in care. Another thing is that hackerspaces accept infrastructure as constantly mangled, open not only to modification but also to interpretation. This instability enables easier experimentation, even on external infrastructures and networks, such as in the case of Speck and Fidel.

This is my other trick. Sometimes, when you cannot see the hack, or you struggle to examine its dynamics, reverse the social optics and think about the care required to ensure reliable infrastructure. Focus on understanding what keeps the mundane possible in order to see the impossible or unusual. It is both a century-old ethnographic intuition and simply common knowledge in the field. If you neglect everyday infrastructure, researching hacking seems hard. This is why the path to computer security is simultaneously so obscured yet so simple. A significant part of the experts I interviewed, perhaps except for academic cryptographers, were ex-developers, ex-testers or ex-administrators. They became members by maintaining the infrastructure. There is a constant flow between SysOps, DevOps, hackers and security researchers.

Research on maintenance is a small subsection in an already small niche in STS (Henke & Sims, 2020). Aside from Star, it stemmed from understanding the differences between synchrotron technicians and scientists (Doing, 2009), office spaces and printer technicians (Orr, 1996) and factory floors and union action history (Noble, 2011), as well as the care of human (Mol, 2002) and non-human (Haraway, 2006) actors.

Not surprisingly, as my study proceeded, Speck and Fidel started doing gigs in security, landing jobs with some solid squads globally. So, before thinking more about infrastructure, I need to discuss the community around Speck and Fidel.

## Evenings in Hackerspace

As the evening passed, a local high school student dropped in to finish some soldering in their homework project with FPGA (Field-Programmable Gate Array, type of hardware with logic reprogrammable after manufacturing, often used in low volume / high customizability designs and in research). System administrators joined Speck and Fidel to discuss the local job market, contract rates and transfers. In other places like this hackerspace, you may

also encounter ham radio clubs, privacy workshops or computer numerical control (CNC) machine shops. Here and today, the mood was more for programmers, architects and developers with more laptops, smaller groups, quieter talk and more intense periods of individual work.

Rush hour in the city ended as evening turned to night. More people were coming and going. Some of them just stopped to say "hi" and to pick up stuff they were storing here. Others met here to speak Chinese in friendly surroundings. Admins and high schoolers sat together discussing a recent zero-day: a newly found vulnerability in some computer system, known publicly as zero-days and so new that system developers were unlikely to produce a patch, solution or any response at all.

I will return to zero-days in Chapter 4, as they are key epistemic objects for understanding computer security knowledge. But even this quick glimpse may lead into a nice sociology of science paradox. A zero-day is an equivalent to scientific discovery, as transferring it requires advanced knowledge and trust. At the same time, by definition, it depends on not being publicly known. You may wish to test your zero-day on targets, to check if it still works, but each test raises the possibility of recognition of and patching against the vulnerability. So, zero-days share the factor of surprise with secret weapons, but they do not necessarily share deterrence properties. Even if they were not part of computer crime or computer warfare, zero-days would still be perplexing as objects of knowledge.

This is why I always felt that a philosophy of science cannot be detached from social practices. Just a few months later, I would learn more about exploits, and I try to compare them with scientific facts, their replication mechanisms and politics.

Philosophical musings are great to vent during breaks, but I have to get back to ethnography. Some people were talking in the local language; others were foreigners who did not have many places in the city to hang out. The things discussed and developed ranged wildly. Some people were engaged in deceivingly simple, extracurricular high school stuff. Others discussed issues from senior development/operations in a bank. Sometimes I willingly chose not to listen to avoid the risk of them breaching non-disclosure agreements.

That is what a typical evening in a hacking community looks like. For a passer-by, it will look like people just hanging out. But if you hang out yourself for a bit, you will notice experiments or discussions about scientific papers. There is a no practical difference between an obscure scientific discussion or an evening hang out with a beer. It's also impossible to tell when maintenance stops and hacking ideas start. "Aha moments" do not happen constantly, so they are easy for bystanders to miss. What matters is that communities formed around maintenance provide enough reasons for hangouts to happen. This is the soil, or silica, where experiments grow.

The results of an experiment do not need to be spectacular or worthy of discussing at a big hacking convention. They could be about preventing a local data leak or even a minor infrastructure error that end users would not

have known of. They could be mundane, not likely to be recorded by historians. Yet, for me, they mark an interesting fact about machines and social relations. Machines can be hacked as a part of casual conversations, not necessarily for malignant, reputational or financial reasons, but to test ideas or as a stage in a larger project.

This means that the infrastructure for hacking consists not only of ways of securing your attempt from outsiders (law enforcement or others) but also of having enough people to chat with about a new paper in sufficient privacy. It means having spare servers to do "quick and dirty" tests. It means having enough free time and other resources to work without immediate results. It means having a place for failures and learning. When I enumerate such things, they may seem obvious to conducting science, in particular, and any kind of creative endeavour in general. Notice how we are moving away from the single hacker, socialising only through online modes. How they are becoming more enmeshed, less universal and more dependent on a communal division of labour.

However trivial such processes may sound, I recommend just paging through the history of post-war particle physics, exactly at the moment when physicists had to learn how to work with electrical and electronic engineers to make better particle detectors (Galison, 1997). You will immediately notice that collaboration in the laboratory is fragile and far from obvious.

Would it be a big surprise if I were to tell you that CERN has a hackerspace and that engineers taking care of circuits in the supercollider almost annually give talks at a hacking convention in Europe?

## Global Causes, Local Dynamics

As digital markets grew (Śledziewska & Włoch, 2021), the need for cheap IT labour grew with them. New EU countries provided a useful outsourcing backbone, first for Germany and the UK, later for the rest of the EU and the USA.

Poland, Slovakia, Czechia and Hungary had cheaper but educated workforces with reasonable knowledge of English thanks to pre-EU educational programmes. These workforces were also mostly free of significant educational debt, as higher education was highly subsidised by the state. This last factor was easy to overlook but proved to be key for the growth of the sector.

A SysOps engineer may be responsible for the maintenance of servers in Germany when working from Czechia, Hungary or Poland. Without a significant time difference, they could work during rush hours without harm to their biological rhythm and without disrupting the organisational rhythm of the company. At the same time, their salary will be 10% to 30% lower. In the case of a critical failure, the workforce is easy to mobilise. Transport from a hub in Czechia to Berlin or Munich (German IT hubs) is a matter of two to five hours by car, bus or plane.

Such a workforce, while more expensive than Indian or Brazilian programmers, was also easier to process with regard to tax, employment and life situation issues. This is why any understanding of European hacking without understanding EU and Schengen Area dynamics is incomplete.

What started with outsourced software testing and administrative labour grew into computer security expertise. This is why familiarity with different software communities contributes to understanding the sociological structure of knowledge in computer security. There are few standardised education paths in this specialisation, so a major source of recruitment is from within the field. University courses on computer science or electronics rarely cover contemporary security architectures or penetration testing.

Why does it matter? Simply speaking, if communities provide soil for the growth of experiments, then outsourcing provided soil for the growth of communities. Later, communities took the form of hackerspaces and specialised as security companies, small academic research laboratories or government security research groups. I will return to the differences and specifics in this ecosystem in Chapter 2, where I will discuss the simultaneous discovery of a very intricate hardware vulnerability.

The ecosystem as a whole had one more soil cultivation mechanism that worked along with outsourcing and the EU's open internal borders. In 2022, the public may have forgotten about its roots, but I cannot. In 2015, when I was moving between different communities in the region, there were two universal topics: American computer intelligence surveillance and EU privacy/digital market reforms. They may have become old news, but they had an impact on politicising hackers. They also changed the structure of computer security professions.

## Evolution of a Privacy Law

Chelsea Manning in 2010 revealed messages between American diplomatic institutions. The messages suggested that American intelligence was routinely wiretapping UN and other foreign officials. The content of Manning's leaks and public reaction to it were primarily focused on military crimes in Afghanistan and Iraq, but, diplomatically, it likely raised institutional suspicions in the EU.

In 2013, Edward Snowden disclosed cables showing that the NSA routinely surveils EU parliaments, officials and citizens (Greenwald, 2014).[4] European politicians and institutions were wiretapped, as were the parliaments and institutions of individual countries. Practically speaking, the EU negotiated trade agreements with the USA as if they were playing with open cards. Heads of state were tapped so routinely that even people extremely cynical about diplomatic protocols were surprised.

In hackerspaces of Central Europe, morbid irony was the common reaction. The absolute majority of respondents knew and assumed from the beginning

that civilian or military intelligence agencies might surveil their communities, as they surveil European governments. They knew about the NSA, and they assumed that my study might be part of an intelligence gathering operation. In one of the communities, they adopted a custom. When I was saying my goodbyes, they would reply, "Goodbye, and our regards to the Colonel". I passed their best wishes to my PhD thesis supervisor (a civilian sociologist and an officer in the Polish army reserves). It seemed that even hackers from the former Soviet bloc had little hope about the protection of individual rights in Western democracies.

After the Manning and Snowden leaks, privacy law reforms in the EU gained new traction with the Data Protection Directive (95/46/EC). They were already different from those in the US, but the leaks brought more attention to the issue. In 2016, the EU introduced the binding General Data Protection Regulation for all digital companies operating in the European market.

As the EU remains a significant consumer market as well as a source of outsourcing and a partner in tax evasion for global companies, other regions followed with similar regulations to ensure stability of terms of trade.

But the history of EU law will not give you the full picture. For the hacker-activists I interviewed in 2013 and 2014, both the leaks and the EU institutional response were not abstract, distant echoes of alien signals sent by stuffy bureaucrats. They happened viscerally during a series of the biggest and most noted hacking conventions in Europe during the studied period. They caused splits in communities and shaped new alliances. I followed hacking communities as they attended Chaos Communication Congress (C3) from 2014 to 2019.

Chaos Communication Congress is so important (Kubitschko, 2015) that I will return to it later to discuss it as a scientific meeting. At the moment, I wish to focus on its impact on communities and outsourcing and how it shaped computer security as a business.

In short, following the hacking community brought me to a European hacking congress. Shadowing just one member of this community brought me into a workshop that connected EU law with the hacking community in new, unexpected ways. The vibe shift is easiest to grasp when you look at Congress mottos. In 2012, it was "Not My Department"; in 2014, "A New Dawn"; in 2015, "Gated Communities". The 2013 leaks made so large an impact that Congress did not adopt any official motto – for the first and only time in its history.

Certainly not all participants and not every hacker in Europe agreed with this politicisation, but every hackerspace I visited from 2013 to 2015 (about 15 of them) was discussing something related to leaks, privacy and surveillance. The mood at the Congress was similar to the mood in the communities, especially in those more political, more anarchistic or more interested in computer security. I personally believe that the leaks convinced some people to participate in my study.

Before I explain relations between EU institutions, I want to say a few words about my research during the Congress. Among many other underground currents after the leaks, it was the Congress that acted as a trading ground between various EU institutions and hackers.

## This Is a Proper Anarchist Conference. We Have Minutes.

I went to C3 as part of a multi-sited ethnography. It was an important event for communities I was a part of, so it was natural for an ethnographer to tag along.

The Congress had about 10,000 guests at this time, so it was impossible to understand it as single event. Instead of stationary observation, I decided to shadow individual hackers, who consented to this. I wanted to see how they shaped the Congress as a personal experience (Marcus, 1995). I mixed shadowing with stationary observations of "my communities" during General Assembly (a place where hackerspaces are open to set up their "bases") and my own personal observations. I learned more than I expected about the EU and hackers during one of the shadowing days.

It wasn't the first day of my application of this method, nor was it my first Congress. Scruffy and tired from lack of sleep, I was shadowing one hacktivist I knew from stationary ethnographies and other Congresses. And I was shocked. Almost half the people there wore ties or comparable business casual attire! In the middle of my Congress? What was that about? The hacker I followed just advised me to listen and participate as capably as I could. "You're not a hacker, but you know something about institutions in the EU and social stuff. Use it at will, you are among friends".

It turned out I had walked into a semi-open workshop very unofficially connected with very concerned analysts from an important EU administration. Not a consulting company, not a think tank, not a research project, but an institution that was in the loop with an EU regulation proposal as it was being drafted. (I do not provide further details to protect their anonymity). Very informally, some people involved in EU policy organised a policy workshop with hacktivists, using the Congress as neutral ground.

The majority of people knew each other from privacy debates on the EU scene or from the anarchist movement. Sharing similar backgrounds, I also recognised some from debates in their countries. I stated my role as ethnographer and asked for their consent; we discussed anonymisation conditions, and the workshop started.

The workshop concentrated on the details of the role of privacy protection in agreements between the EU and the USA. Both policy geeks and hackers were aware of American intelligence activity in the area and discussed data protection standards that needed to be enforced. I was no stranger to privacy debates, and I broadly understood terms from public debate such as "safe harbours", "Five Eyes alliance", "public key mechanism", etc., but the workshop went much further. The level of technical complexity in law – its institutional

and technical aspects – was much above anything I had experienced in academia, the public sphere or anywhere else. Again, I agreed not to disclose exact details to allow anonymity. I tried to contribute as much as I could when cases from my domain were discussed.

I brought examples and sources on privacy protection standards in social research and data-sharing mechanisms I had learned about when I read about different cultures of access in different scientific fields (e.g., standards in European particle physics may differ from those in European meteorological collaborations, even if some supercomputers and other resources are shared. It's something obvious to people in the fields – things you learn just from hanging around climate scientists or reading the basics of synchrotron research. It is easy to overlook when discussing policy regarding data in general).

After the workshop, the hacker who led me here said that it was exactly what they were looking for. We provided better cases for EU institutions who will be supporting negotiations with the US. Of course, both of us were usually paranoid, so we did casual background checks on a few newly met analysts and activists. Nothing shady, more a matter of a professional curiosity and habitual fact-checking. Just asking around friendly squats by email, checking the publication records of people we met and the university history of some analysts. People from the workshop held up to this scrutiny.[5]

Apart from the resemblance between understanding complex software and understanding complex social systems, I think this workshop is important to note because collaboration between EU hackers and EU institutions is not recognised in the research. It is public knowledge in the field that US officials engage in similar work. For example, the commander of an American computer espionage agency delivered a famous and widely criticised keynote lecture at Defcon in 2013. An American military research agency (Defense Advanced Research Projects Agency – DARPA) conducts experiments in machine learning during conferences on a regular basis. European hacking conferences are usually seen as much more left-leaning and politically radical, due to their roots in the German hacker-anarchist movement. My colleagues researching hacking in Europe focused on national levels, such as the impact of hacking on German politics (Kubitschko, 2015).

The workshop I encountered proved that there were efficient links between EU policy institutions and hacking communities – links which bypassed national administrations and public, civic society mechanisms, instead making use of the obscurity of Chaos Communication Congress.

A second conclusion is more hypothetical in nature, but I feel it needs to be stated openly. I argue that it is reasonable to believe that some hacktivists were likely active in shaping the EU's General Data Protection Regulation. When I hypothesise about this activity, I do not mean through providing illegal access to communication networks, spreading leaks or organising dissent. I mean providing expertise to EU analysts and law researchers – not through lobbying, think tank activity, policy papers or other forms of public advocacy.

A set of changes associated with GDPR was developed on multiple levels, both within and outside European Parliament. What is important is the fact that GDPR affected countries beyond the boundaries of the European Union. This form of extending the range of political power by the combination of law and software standards was called "the Brussels Effect" (Bradford, 2021). Only recently has research in social sciences recognised its effect not only in global digital trade or international relations (Eskhita & Stamhuis, 2024; Ylönen, 2025) but on the profession of cybersecurity (Birnhack & Mundlak, 2025). As an ethnographer, I observed how EU's bureaucrats held "public" consultations during Chaos Communication Congress, one of the biggest conferences connecting cybersecurity and hacktivism. As I contributed to some workshops on the issues related with public understanding of science, I was asked not to give any more details.

EU regulation directly interacted with hacking communities and cybersecurity professionals. Since 2018, security leaks with European citizen data are no longer just a public relations problem. They can be a source of serious financial fines, as imposed by national administrations. The business incentive for data protection is rather strong, as a potential fine for data leaks may be up to 20 million USD or 4% of the annual income of the company. Simply speaking, disregarding data policies may become much more expensive than spending more to improve security.

As a result of privacy regulations, the data protection sector grew almost overnight. This is why I consider understanding hacking communities without knowing EU institutions as incomplete. This is also why I think that a policy workshop in the middle of a hacking congress challenges our understanding of issues of law, science, technology and institutional practice.

In this chapter, I have discussed elementary experiments (like the one discussed in Interview 1.2) undertaken in hackerspaces in Central Europe. I have discussed the factors that affected the growth of interest in computer security after 2013, including the rise of IT outsourcing, as well as leaks and shifts in EU policy. I have argued that, similarly to scientific laboratories, informal research groups such as hackerspaces serve as potential resources for European policy as well as local sources of know-how for the maintenance of infrastructure in commercial companies.

It is time to reveal more elements of the puzzle. How do academic laboratories around computer security work? How are hacking communities connected with professionalised computer security? Perhaps after learning about these issues, we will be able to finally figure out the details of sociological mechanisms in computer security laboratories.

## Summary

Perhaps, reading this chapter evoked some of my personal experiences from the ethnography. Instead of an linear road, the chapter as well as the

Let's have a look at this cheap electronic gizmo. It's just Wi-Fi and an SD. Originally it was for extending the capabilities of a smartphone, adding, for example, extra memory without the necessity of modifying the phone. Two separate black boxes, designed to achieve specified goals. Hackers who described this online [online source anonymised] said the low cost of the circuit means that the costs of failure are acceptable and little has to be spent to ensure the security of the construction.

One of us discovered that you could log in to the control unit of this device by using a simple password. They also tested modification possibilities with rudimentary programming tools. See the first irony of black boxes: standardised black boxes enable standardised tools. Standardised tools make hacker work easier. We did not have to reconstruct the internal logic of the device nor create our own interface to modify the control system. They described the way on the source I mentioned and so it worked.

A few months later, two of us looked at the physical construction of the device and added new connections. They used exposed access to some circuits. They also modified controlling software and added new functions. They also described their hack on a public repo (repository). This repo was quoted on Hackaday page, for lulz [laughs] and the joy of other members of the space.

So, the modified gizmo may now function in new ways, including increasing privacy in some venues of hacktivism. It could also be used in simple projects with distributed computing. Later editions of the original device had updated software and hardware architecture, so we had to update the description of our modification.

*Fragment 1.2* Narration about a "good hack" performed in the hackerspace by two hackers. The hack was recognised globally and became as source of joy for the whole community. The narration is from an unstructured interview. I have concealed details to protect anonymity and cleaned up the written transcript.

ethnography resembled seeing through a kaleidoscope. Singular pieces were more or less complex on their own, but what really fascinated and lured me into the next step was their interoperability and complexity, as understood as another layer over the pieces.

This allure and wider-picture understanding is exactly what I think that cybersecurity experts seek when they say "I have a root". It means not only having a control over the system but also thoroughly understanding it. Of course, I claim no control over system of cybersecurity over global scale and even my claims over knowledge are limited. Having that in mind, I tried to

evoke this experience not in terms of scale but in terms of joy, discovery or confusion. In other words, through the medium of ethnographic text in this chapter, I attempted to convey the very specific experience of the multitude of breadth and perplexity of topics that the cybersecurity expert may be asked to handle. Similarly to kaleidoscopes, cybersecurity problems and my study of cybersecurity as well, will have many moving parts that will constantly change meaning as new movements will be made. This chapter evoked the sensation of understanding, of perplexity, of allure I found as a broader pattern among individuals and groups.

Moving on from evocative to more analytical conclusions, I wish to underline a few issues. Firstly, it is sound to note that some hackerspaces, and similar groups I described as non-formal, do not constitute a majority nor representative sampling for cybersecurity research groups in the field. Having that in mind, I believe that it was not previously reported that the hackerspaces acted as a network nodes contributing as attractors for expertise, translators or mediators of activism in civic society processes at the transnational scale of the European Union in the case of General Data Protection Regulation (GDPR). This is the crux of my argument: if for the case of GDPR, as well as for others, the expert knowledge from groups like hackerspaces was recognised as important, even if in less than public circumstances, then I argue such groups are recognised as sources of expertise in the field. This is a sociological definition of a science: a publicly recognised and legitimised source of expertise. In short, if groups like affiliates of hackerspaces were reached by some EU aides as sources of expertise, then I argue that groups like hackerspaces contribute to circulation of knowledge that is recognised as scientific.

By "recognised as scientific" I do not mean affiliated with academia or given the similar prestige or social credit as disciplines like biology, medicine or history, but reached as a source of expertise, objectivity, efficiency or any other positively associated values that given society or its delegates associates with sciences. In other words, this is legitimisation by the para-state apparatus (EU is not a state per se!), but with very little public recognition. Readers should not put too much emphasis on the "hackerspace" part nor on the "EU" part because there are more than plenty of examples of non-hackerspace groups that contributed to the expertise of state institutions. I will discuss more examples further in the text.

A second conclusion is an implication of the first: the cybersecurity knowledge and social underpinning for scientific discoveries grow as much from the military or intelligence supremacy as from maintenance and subcontracting.

This is what connects hackerspaces, EU aides, corporate security labs and many other groups in a field that is understood as a science of cybersecurity: not only the issues, practicalities, inscriptions and so on but the knowledge and power to integrate and delimitate them over the next layer. If physics is obsessed over the infinite regress over time and matter, then the cybersecurity obsession lies in constructing, weaponising and exploiting abstraction over

abstractions. This is the kaleidoscope libidinal mechanism, this is the dialectic in motion, this is the connection between the knowledge of the attacker and the knowledge of the defender. This is the "irrational", or to be more polite, the emotional or passionate part, of the science, the part that is felt among and within the practitioners and that is translated through the invisible curriculums, through mentoring and through the most private of gathering. This is the cognitive "kick", at least for those researchers who seek epistemological rewards.

If the metaphor of the kaleidoscope is overextended, does it become a theoretical bypass? Either way, starting with the notion of infrastructures, through the global division of labour in maintenance and subcontracting, as revealed through groups like hackerspaces, thus catalysing knowledge recognizable by trans-state actors, I found out the "kick", the libidinal or the dialectical component of the science. This is the preliminary, simplified and rudimentary introduction to the sociology of cybersecurity.

## Notes

1 Look for music like: DJ Rush – Tetris Russian Theme (Techno Remix) or Complete History of the Soviet Union, Arranged to the Melody of Tetris. Then play it on loop for four years.
2 In this example, as well as with all examples, details are anonymised. This was a condition for consent that I proposed to the participants. This is why I was able to learn what I have learnt. This is also my sign of respect for the cybersecurity as a field, which in general, places a special emphasis on privacy and trust.
3 Science, Technology, Society – abbreviation for the broad field in social sciences and humanities. Alternatively, the same abbreviation is understood as Science and Technology Studies. The later is more inclusive for non-sociologists, while the former slightly more emphasises structural considerations and understanding of each component as semi-separate, but complex, interlocking and overlapping etc. As a sociologist, I situate my practice closer to the understanding as given in the former, while as a researcher I staunchly believe in inclusivity of the later.
4 I do not agree with moral, ethical and professional standards proposed by Glenn Greenwald in 2022, either in gender or in international politics. In addition to that, I wish to note the critical contributions to journalism and operational safety of Snowden's materials made by Laura Poitras, Jacob Applebaum and Barton Gellman.
5 With hindsight, I must admit that I developed a habit of double-checking in Google almost any intellectual, activist, security specialist or civil servant who takes interest in my work. Most likely, I picked up this habit after doing background checks after this workshop.

# 2 "Groups."

## Laboratories. Profession. Thought Collective.

In the previous chapter, I presented how hacking communities conduct experiments on shared infrastructure. Such experimentation allowed them to participate as "silent experts" in the development of European Union legislation, through informal delegations of EU Parliament aides to squats and hacking conferences. Of course, hackerspaces are not the only communities that bring together cybersecurity researchers, nor are they the only groups that are sought for their expertise. In Chapter 4, I will discuss the case of Citizen Lab and of its uncovering the use of the Pegasus surveillance system against political opponents in Poland and in other countries of the EU.

In order to develop a conceptual framework that goes beyond a list of case studies, I need to do some sociological DIY in terms of theory. By this, I mean explaining sources, adaptations, reach and evidence for use of terms I had chosen. While those words may be familiar from everyday language, from science jargon or from introductory work in science studies, I kindly ask for some attention.

Thought Collective. Profession. Laboratory. Those concepts may sound simple, but each of them was a subject of discussion in my field. I believe that there is scientific value in precision, delimitation, understanding and reference to prior research. Exactly for those reasons, I will not be rediscovering the wheel, but I will instead examine, modify and validate against my research. Since social concepts may be overwhelming, I provided an overview in Table 2.1.

### Laboratory. The Context of Discovery.

The laboratory is the smallest of the cybersecurity groups that I am interested in. It should be noted that a laboratory is not the same as authorship. A multitude of vulnerabilities have singular authors, but to consider their cognitive operations as solitary is to follow the siren's call of classical philosophy of science: once again heroic narratives of singular geniuses, self-made men. Such image is the long shadow of romanticism or science propaganda for

DOI: 10.4324/9781003396871-3

*Table 2.1* Three sociological concepts for understanding cybersecurity

*Laboratory allows for recognising differences and similarities with other sciences while also providing sociological insights into burnout of individuals, the role of support staff and career mechanisms. Profession allows for understanding of ethics, autonomy and interactions with the state. Thought Collective, while similar to a paradigm, includes the hierarchy of insiders and communicators.*

| *Concept* | *Laboratory* | *Profession* | *Thought Collective* |
|---|---|---|---|
| Definition | A group of people that facilitate discovery by reducing costs of failure. Discoveries have to be recognised by actors outside the laboratory. | A group of people bound together by specialised knowledge, public trust, public prestige and a code of ethics (formal or informal) | A large community of people bound together by exchange of ideas or intellectual interactions. |
| Examples of questions | How do cybersecurity researchers collaborate in everyday basis?<br>What do they need? What should a research group have in order to do continuous research? | Who has jurisdiction to conduct cybersecurity research, and who would be regarded as a hacker?<br>What counts as research, and what counts as a breach of intellectual property?<br>Who is called to judge other cybersecurity professionals? | What cognitive traits were shared and what differed among cybersecurity researchers who discovered the Spectre and Meltdown family of vulnerabilities?<br>What was the shared trait among different generations of hardware engineers who overlooked this? |
| Scale | Several people. Everyday contacts and collaborations. | Nation-states, with some exemptions (big corporations, military alliances, etc.). | Global, beyond the boundaries of singular funding agencies. |
| Sources in Sociology | Bruno Latour and Steve Woolgar (1986), Harry Collins (2017), Karin Knorr-Cetina (1999), Izabela Wagner (2011). | Max Weber and others, but my definition takes from Andrew Abbott (1988). | Ludwik Fleck (2008). |
| Relevance and author's interpretation | Laboratory allows demarcation, which is separation of research and researchers from the outside world. Then, within the laboratory microcosm, researchers may ask otherwise unacceptable questions (is this obvious fact really true?), go against social norms (cause discomfort or harm in order to do research) or otherwise put social norms on pause in order to reconfigure epistemologies. | Establishment of legal standards, ethical procedures (e.g., responsible disclosure) and development of the public understanding of the field signal that the particular field achieved autonomy and prestige. Autonomy means that legal and state apparatuses require somebody from within the field to judge the professionals (e.g., a judge requires a medical expert to judge a medical malpractice case). | If a field of science achieves coherence enabling the formation of thought collectives, then socio-cognitive phenomena like incommensurability and simultaneous discoveries occur. Thought collectives signal social formation of "big science" (Price, 1971) and formalisation of the field. |
| What domains are related? | Philosophy of science, sociology of scientific labour, science studies, scientometrics, management. | Law, ethics, military sciences, political sciences, sociology of labour, public understanding of science, HR. | Philosophy of science, cognitive sciences. |

IPO investors (a brave self-made poet, inventor or investor), but it is not the sociology of science.

My conceptualisation of laboratories is built on works of Bruno Latour and Steve Woolgar (1986), Harry Collins (2017), Karin Knorr-Cetina (1999), Izabela Wagner (2011) and many others. The advantage of this approach was that I looked for similarities in everyday research work in other disciplines: funding, correcting publications or equivalents, reacting to advancements in the field, career trajectories, etc. The downside is that by making such broad-scope comparisons, one can easily forget that each of the referenced works was also situated in particular context of its time, institutional setting, research field, etc. The challenge in conceptualisation of the laboratory lies in understanding similarities, without reification, which is a fancy word for treating some social characteristics as natural, unchangeable and eternal. As a sociologist, I am as distrustful of reifications as security researchers are, because what is left unsaid as obvious is often simultaneously the most binding and most fragile of the components of social structure.

This is why I wish to be precise. Not every collaboration is a laboratory, and not all discoveries have to originate in a laboratory either. I introduce the concept not to explain everything, but because it shifts some attention to the changing scale of collaboration in cybersecurity.

As Steven Shapin and Simon Schaffer (1985) or Harry Collins (2017) painstakingly documented, establishment of laboratories signals a certain degree of specialisation, in terms of measurements, techniques, calculation or experimentation. This is also why I believe that careful understanding of laboratories *as social structures* is key for answering questions about cybersecurity knowledge.

What was important for my conceptualisation from Shapin and Schaffer (1985) and from Collins (2017) is the redefinition of the demarcation problem from a domain of philosophy to the domain of social practice. In other words, to answer what is cybersecurity as a science, one has to answer what doesn't count. Yet, as a sociologist, I am less interested in asking this question in general than in attempting to develop how this question is understood by practitioners. Thus, my conceptualisation: the laboratory is a site and a community of demarcation because, only on this exact scale, decisions are made about what to count as noise and what to include in measurement.

On a side note, by this point of the book, it should be clear that my usage of "laboratory" is not aimed to separate "academic" or "scientific" cybersecurity from "practical" or "hacking" or "illegal" or to create any demarcations as a part of my conceptualisation. As a sociologist, I observe that the cybersecurity uses and is used to demarcate various other social structures and institutions, but that does not mean that I accept those demarcations as "objectively existing". As mentioned in the introduction, the benefit of the lens of both science and work is that I can freely disregard the divisions between state, private, criminal or non-formal actors. In the context of this book, a well-funded

academic group may not be called a lab, if it does not reduce costs of failure for its members through the mechanisms I describe in this section. Contrarily, what could be easily considered illegal, unimportant or local knowledge at best, I may theorize as a lab. For the scale of the given community, this was the social setting for reduction of cognitive, ethnical or material consequences of failed experiments as recognized by actors in a given community. For me, as a sociologist, the science is inextricable from the society that uses it.

For example, Jonathan Spring and Phyllis Illari (2025) asked a great question about whether cybersecurity has an equivalent of experiments, understood as isolated test beds of cases that are differentiated through interventions

| | |
|---|---|
| *MZ:* | **You hacked it?** |
| *Researcher:* | It wasn't even hacking. Because it was only later that I discovered that it was basically a rework, but disassembling a Windows program into code and reading the code is very easy, as it turned out. But . . . well, in XYZ, fortunately, we are not at such risk, while in the US, the company could possibly be prosecuted for such an approach, because the code is intellectual property. |
| *MZ:* | **Because it is in the open?** |
| | Yes, exactly. I mean, I don't know if it is, it could be. In any case, the code, they could already pick on it for that. I say, in XYZ, they could do little to me, but in America, potentially they can, so I didn't do it. It's not my creation. It's just copying their code, and the code is theirs. |
| *MZ:* | **Outside fair use?**[1] |
| | Yes. So, what I had to do as a result and what I did, I believe that this is the only way. I just started eavesdropping on what was going on the USB cable and basically, okay, I clicked on an interface button, what was supposed to be done was done, that is, an option was activated on the <next device> and something flew along the cable, a piece of these commands being responsible for what I instructed. |

*Fragment 2.1* In this fragments, a cybersecurity researcher speaks on the intricacies of their research. It was not necessary to attack any security mechanisms of the system that was of the interest. It was enough to laboratorise or to enclose the system to have full information about its inputs and outputs. By disassembling fragments of the code and by controlling the inputs and outputs (blackboxing), the researcher was able to find out what they needed. In this sense, the researcher operated in a social setting (unmentioned in the fragment) but laid down the second order of laboratory, a software one, on the analysed object.

and that can be later generalised. As Spring and Illari show, practices known in cybersecurity as threat intelligence can be understood as non-experimental, that is, knowledge as coming from observations. As with many great questions, I have an ambivalent answer. On the one hand, I recognise different practices in cybersecurity as clearly following a separation-intervention-generalisation pattern, from which I claim that cybersecurity encountered issues not unlike experiment replication. On the other hand, please note Fragment 2.1. The interviewee is an experienced and acclaimed cybersecurity researcher. The interview is about a relatively small project that focused on a system that was out of the commercial use. The interviewee researched it, with collaboration, primarily for personal interest.

Notice how careful is interviewee in their contextualisation: what can be counted as hacking, what was more akin to "fair use" and what could be a subject of a lawsuit. It may sound obvious, but, for the purpose of knowledge, the difference between a hacker and a cybersecurity researcher lies in legitimation rather than anything else. A laboratory is thus the social structure that helps in building this legitimation.

Notice also another peculiarity. While the interviewee does not claim that they are experimenting, they are enclosing the studied system to measure outputs and inputs. There are two layers of dialectics embedded onto each other. On the one of the dialectical tensions, the cited researcher is untangling what was reified as coherent but opaque system. On the other, they are making their own work as a susceptible to reification, as any scientific measurement has to exclude some of the author's subjectivity. Tensions within each of the dialectics and tension between the dialectics create what Bruno Latour conceptualized as Janus-faced science (Latour 1987): science is always caught in tension between erasing unnecessary noise and uncertainty about erased data, including thin margins between genuine anomalies and personal biases. For many years STS followed Latourian description, which carefully masked its inspirations in critical tradition. This is why what Maxigas and Söderberg (2022) reconceptualized as dialectical current ever present in hacking, I trace back even further, following Andrew Feenberg (2015), Mikołaj Ratajczak (2020), Andrzej W. Nowak (2016) and many others. Dare I say: set of tensions between and within the system of type one statistical errors and type two statistical errors as shared among many measurement sciences is the drama of reification and alienation. It is not specific for a science as a social activity or as a form of labour, but in science it has its clearest exemplifications. Risking allegory: the most Brechtian staging of concepts of alienation and reification is exactly this thing called science.

What was too long for this fragment was the information about the reception. The research done by the interviewee from Fragment 2.1 was met with a response. It turned out that by showing the presence of some architectural traits and by showing the workarounds, the author pushed forward the studies on emulators and computing history preservation studies.

What other functions can be investigated through laboratories? What new perspectives are opened up by my reinterpretation of the term? Firstly, the

laboratory is a place of work. This is to say that if one is seriously considering cybersecurity as a science, then as a logical conclusion, one should compare cybersecurity researchers to scientists in terms of burnout, the Matthew Effect (exponential distribution of citations), the Matilda Effect (erasure of female and minority researchers), patterns of career coupling (feedback in careers between mentors and mentees) and many others. The tools and concepts already exist. Research on cybersecurity cadres does not have to reinvent the wheel.

If there is a simple model of laboratory, then one may start with the Latourian model of circulation (2000). Please note that I am already presenting my reconceptualisation for cybersecurity because the original text is still accessible. When investigating reduction of the costs of failure in the laboratory, one should investigate five circulations. Four of them operate on interfaces demarcating the laboratory and the external world, while the fifth works as an internal mediator between the first four. Four circulations that transpire and demarcate are autonomisation, public representation, alliances and mobilisation. The fifth one can be called simply laboratory labour.

Autonomisation is the process through which the laboratory facilitates not only discoveries but also researchers who work in it as valid. In other words, autonomisation provides justification for recognising discoveries and researchers. This is the system of credentials but also visible and invisible networks of citations and the mechanisms of vetting and backfire, which is doubly valuable for a field like cybersecurity when there is a public assumption that not everything can be put in print. This is also the gossip network, the lending of honeypots (lures for testing potential attackers and their scenarios) and various other forms of unwritten knowledge.

I will theorise on public representation more in later chapters, but for laboratories, this is important, even if in-group experts do not care about communication with out-group laypeople. Public representation matters because it creates what is understood about the lab by the customers, politicians, collaborators from different departments and new candidates. Finally, the social fact that hacking carries certain cultural connotations may not represent the actual practice of the profession, but the same social fact still influences emotions, values and aspirations of the practitioners. As it is well-known from other sciences, even seemingly positive images of an elite field, full of brilliant people with wizard-like powers becomes a burden when one's research fails. Thus, the laboratory is often the most immediate social group of reference for handling this external, public pressure.

For alliances, cybersecurity laboratories are even more problematic than physics or oceanology ones (Oreskes, 2021). For physics, it has been established that different countries certainly shifted boundaries between science and politics (Wolfe, 2018). When it came to funding, physics was necessary for national survival. When it came to ethics and moral hangover, invoices signed by the military were disregarded as "politics beyond the lab" or "mere engineering". Of course, cybersecurity is also researched outside the

military-capital complex, but any serious sociological work on cybersecurity should take into consideration that, at least until the AI boom, the intelligence agencies were said to be the most common employers of maths PhDs (no singular source, popular belief told by interviewees).

Mobilisation is about resources. Not only money for wages but also computing power, water and space. There is also access to studied systems and access to isolated environments, in which malware may be tested. In some cases, it may mean heaps of old laptops that could be infected, only to be later investigated with disassemblers and oscilloscopes. Similarly to epidemiologists, it is far from obvious that cybersecurity researchers have access to the studied system. Even less obviously, the generation of an attack or hardware in the lab may not be representative for a broader population. This is why mobilisation involves access to old documentation, forks (different branches of versions, sometimes abandoned earlier) and even personal communication with developers. To give one example, in the recent pandemic, reverse engineering of protective respirators enabled extending their supply (Chaari et al., 2020) during the first phase of the COVID crisis.

Autonomisation, public representation, alliances and mobilisation in practice blend together in the fifth circulation. A well-oiled lab tries to maintain a careful balance between "public hours" and "private work", this is, the balance between responding to outsiders and their needs and providing supportive silence, isolation and concentration. Different people have different cognitive preferences and research temperaments, but a few supportive concepts that may be helpful can be taken from cognitive anthropology and philosophy.

In summary, laboratories are the social contexts in which "what is not known" is turned into "what is well-known". This operation requires labour, resources, time and boundary work. It also involves demarcation of issues that would be "too political" to be considered a part of the field and issues that have to be taken into consideration but cannot be described explicitly in the written documents, from open secrets in the field to silent pressures of the power elites. The laboratory is the exact place where failure, doubt, result and discovery go through their first socialisations, moving from the mind of an individual to knowledge usable by groups. Not every working group in cybersecurity is a laboratory and not every institution that has this name is worthy of it, as per my definition.

Cybersecurity laboratories are somewhat unlike many other laboratories because of their particular subject. While many other laboratories, in fact, play an active part in constant reshaping of social norms, boundaries or institutions (think cardiovascular health labs, which provide state-level recommendations, or economic labs, which forecast, underwrite and make mortgages), cybersecurity labs are particular because they essentially can defragment not only the social fabric in the long run and in theory but also sciences, knowledges and practices of other laboratories. This is the paradox I will discuss in further chapters: attempts to systematise cybersecurity as a science rightfully understand that cybersecurity is a science in the presence of an opponent.

However, even at this point, it should be clear that, by developing science in the presence of an opponent, cybersecurity is developed as an opponent for other sciences. Not because it needs fundamentally opposing goals, but because cybersecurity allows casting doubt, noting errors and causing a lack of closure in the research of others.

This is the double-bind of cybersecurity laboratories. As they navigate technical, social and individual stakes of errors for researchers within its field, they also may be of service for jamming, fragmenting or otherwise interrupting laboratories of other fields. If one assumes that cybersecurity is specific because of its presence of an opponent, then it is both a practical and theoretical conclusion in sociology: as cybersecurity develops a laboratory structure, it becomes a dialectical interplay, a counter-lab or opponent for non-cybersecurity labs.

## Profession. Context of Actions.

If laboratories provided context for the unknown, then the profession serves as a collective bargaining mechanism with the state and other actors. Andrew Abbott's (1988) *The System of Professions* tracked the development of medical, legal and accounting occupations into what sociologists call "professions". The key difference between the latter and the former lies in competition over jurisdiction, which is a conflict over the degree to which specialists in the given field can make rules for this field. If it takes other lawyers to accept a person to a bar association, then a profession exists. Medicine, accounting and law developed areas of occupational monopolies for defining, judging, recruiting and excluding their practitioners.

At first glance, cybersecurity looks like a wrong case for a profession. In the majority of nation-states, there are no equivalents of bar or medical associations for cybersecurity researchers. While I have not conducted a full legal review, in my conversational knowledge in most of the Global North, cybersecurity regulations are far from their counterparts in accounting, law or medicine. There is a good case to doubt whether social structures in 2025 can form that kind of middle-class interest lobbing, as tracked by Abbott in the 19th and the early 20th centuries. Social patterns are, after all, always embedded in their time.

Instead, I will offer a description of cybersecurity research that convinced me to think otherwise.

At the end of 2023,[2] a group of cybersecurity researchers communicated that the propulsion failures of Newag Impuls locomotives allegedly can be explained by the mechanisms of failure planted by the manufacturer (*Breaking "DRM" in Polish Trains*, 2023). The group consisted of three researchers: Redford, q3k and MrTick. They described themselves as "loosely affiliated with Dragon Sector", a Capture the Flag team (for more on CTF, see next chapter).

The researchers were hired by a railroad maintenance yard, which has won a contract to service Impulses that run in suburban and regional rail lines.

Initially, the yard proceeded as it was a locomotive maintenance issue. It performed repair, replacement and other services, as per producer's manual. However, despite the "normal" railroad work, the locomotives declined to run again. There was also no pattern in their failures: some of them failed after only a few hundred kilometres, and there was no clear record of heavy weather, heavy load or abnormal rail operation or signal conditions. Typical "suspicious" mechanical parts were serviced and re-checked once again. When even this failed, ZNTK decided to commission an inquiry in matters of cybersecurity, industrial automation and its relation to software and hardware. The inquiry was contracted to a group affiliated with the Dragon Sector, a cybersecurity e-sports team, because Dragon Sector was highly regarded for their skills, especially in reverse-engineering (Haertle, 2023).

I will not reconstruct the technical and legal aspects of this case. Firstly, because court proceedings have not yet finished, and, secondly, because a separate paper is being prepared. Rather, what is important in the context of our discussion of profession is the following: by bypassing security mechanisms of brakes, engines and other parts of industrial automation; locomotive navigation systems; and its main bus (an element of the digital architecture for transferring information), the researchers – allegedly – found out that locomotives that failed were distinct by having code fragments that told them to "brick" (stone-cold disengage after a stop) in very certain places, after specific travelled distances or under various other conditions. This was the allegedly missing link: not the final material effects, which varied, but the malicious lines allegedly embedded into deep layers of the locomotive systems coding.

As researchers delivered results of their inquiry to the yard, the locomotive's manufacturer reacted with a counter-claim, accusing that it was, in fact, the researchers who planted the malfunctioning elements. According to the producer, their interest was clear. Because ZNTK was unable to fulfil the contract for servicing the trains on time, it was necessary to rely on conspiracy theories and plant some evidence for them.

The whole saga of Impulses is long also because it had a sequel in civic lawsuits, parliamentary hearings and the involvement of NATO's and Poland's intelligence services. Researchers also made a public lecture on the legal counteractions and the emotional toil that it took on them (Kowalczyk et al., 2025).

In the middle of all this complexity, two things captured my attention. The research team, from the beginning, established evidence protocols akin to ones used when other sciences are called to serve the bench (see Albright et al., 2023 for discussion of history and tragedies in the United States of America, which exports surveillance and cybersecurity software to other nation-states). The researchers carefully maintained the documentation and kept track of the separation between what was the original system and original data obtained from the locomotives and what was the samples and data used for experimentation.

Imagine the toil. Granted, you and your mates may be cybersecurity researchers, but you know each other predominately from what is essentially

an e-sport. Now you have to do bookkeeping in parallel with all the fun, engaging and intellectually satisfying riddles. Without documenting what was the component of the locomotives and what was set up to conduct the reverse engineering, tests and security bypassing, the results may turn out worthless. I cannot see it as anything other than the equivalent of experimental and reference samples. This is cybersecurity science in the making.

This is also what is at stake in this case. If the civil suits were successful, the researchers would be understood as hackers. Their research would be deemed an intrusion, and there would be no separation between the object of study and the particularity of their method. In other words, if laboratories had to deal with demarcations in knowledge as done through cybersecurity and understood within cybersecurity, then the profession is about the autonomy (and hegemony!) of the field's conclusions in legal, state and other institutional systems. Freedoms to establish bar associations, ethical codes, state exams or university curriculums are consequences and epiphenomena but not the causes.

This is also why this case convinced me to state the hypothesis on the formation of the cybersecurity profession. Because the Parliament, the intelligence services, the courts seems to have accepted the evidence as presented by Redford, q3k and MrTic, this acceptation serves as a benchmark and an example of social proof of "good enough science" in cybersecurity in a public eye. In other words, powerful state actors in broad daylight attested that the evidence procedure for distinguishing between "what was prior" and "what was used in research" is good enough. As manuscript of this book is submitted, researchers have not been found liable in any civil suits. Cybersecurity was allowed to conduct its own research in Poland, and the European Union seems to recognise it as within the "right to repair" and within the public interest. What was jarring was the polarisation between some of the press discourse and the professional responses (Atack 2023; Q3K 2024). Researchers faced a press campaign that followed the lawsuits, while the professional discourse was nigh uniform in support for them. I believe that what was at stake was the recognition that sometimes it is within the public interest to maintain the freedom of research in the realms of technology.

Andrew Abbott reconstructed that professions emerge because they successfully convince public that it is in its best interest to give away some power to the experts, who have specialised knowledge. That was, of course, more of a narrative justification than cause because details of power are very rarely so clean. However, Abbott also recognised that as a consequence of such justification, professions develop ethics and methods of in-group regulation.

Of course, the history of the 20th century shows that medicine, law and accounting committed more than their fair share of crimes against fellow citizens. This is one of the reasons why it is understood that insight of the professionals is necessary but not sufficient to monitor their field. This is also why my conceptualisation of a cybersecurity profession is a way of recognising that cybersecurity specialists are not only involved in spying, defending or surveilling, but they also constitute a next stage in what Allison Powell called "hacking in the public interest" (Powell, 2016). When such hacks become so

sophisticated, so well-documented and so resembling scientific experiments, then perhaps a profession is being born. Not from its power over laypeople but as a form of a public service not dissimilar to the oversight performed by sciences, arts and media.

My claim on professions is not based on my normative hopes. One case from Poland is not enough for the European Union, nor to extrapolate for the world. So, what are the other reasons for the concept?

This is the second reason I use this concept. This may be my next research project, but I believe that the standards in cybersecurity profession are on the rise. My exploratory research suggests that the need arises from the rising costs and consequences of ransomware as well as the militarisation of digital societies in general. This is the difference between a cybersecurity professional and a layperson: insurance against ransomware for systems developed by the former is underwritten more cheaply than those by the latter, so the work of the former has to be controlled, certified and subjected to a different regime of liabilities. This is the aikido of securitisation: if processes of systematisation and professionalisation make cybersecurity more and more accountable to an appropriate sector of the insurance industry, then public, civic and democratic oversight mechanisms have some ways to follow. It is a faint hope, but it is still worth articulating.

## Thought Collective. Context of Scientific Knowledge.

If "laboratories" constitute the context for everyday research and "professions" constitute the context for evaluation of research by the public, state or legal system, then the "thought collective" is the most general "state of the art". This is what is known to the community of generalised peers, what is deemed absurd, what is understood as a common threat and what would constitute an epochal breakthrough. This is why I insisted before that the laboratory results have to be received by a broader research community. The thought collective is this community.

For some readers, this concept may seem similar to the concept of scientific paradigm by Thomas Kuhn (2012). This is both a helpful and a misleading association. Helpful, because the concept of a thought collective was proposed by Ludwik Fleck (2008), a Jewish-Polish epidemiologist and a philosopher of science in interwar Poland in 1930 (Sady, 2023). A thought collective, similarly to a scientific paradigm, emphasised the socialisation of students into the occupation by learning how to read errors, learning how to operate measurements and learning to occupationally disdain some data points as random errors while deeming others as interesting and crucial.

A thought collective is what sociologists call "social facts". This is to say, it is a useful simplification and an abstraction. I do not claim that researchers belong to some sort of hive mind or that they share some sort of

subconsciousness just because they share the misery of doing cases from the same textbook. This is exactly the difference between Kuhn and Fleck in my reading. What Thomas Kuhn invoked in psychology of Gestalt, I reconcile with the shared genealogy of Western science. My bet is that a hypothetical cross-generational study on reading a hagiography of Feynman would explain more normative declarations, or at least nostalgia, about science than any large sample studies on Gestalt forms.

A thought style is a generalisation at the level of a very large group. An individual takes part in elements of this generalisation by a sub-abstraction called a thought style. This is the point at which my interpretation differs from the usual. I associate the thought style with individual humans but not with cognitive ways of a thought collective in general.

In the scale of a laboratory, thought styles of individuals have many shared properties, such as dependence on a particular intellectual tradition or a preference for some tool or calibration method. In the scale of a collective, other intellectual traditions, tools and methodological approaches are recognised, although some may be more dominant than others. The difference between a laboratory and a thought style is the difference between direct collaboration and indirect familiarity.

This difference also covers aspects of cognition that could be on the verge of consciousness: what will be seen or missed in a computer code, what memory logs will go unnoticed, what elements of thousands of pages of manual of hardware will be examined first. A non-insignificant part of a thought style is learned through socialisation, although often in a tacit way and in non-formalised formats (Collins, 2013).

What is important is the fact that a thought style is both a way of insightful seeing and unseeing of unnecessary noise. If one wants to examine any complex issue, no matter whether it is a locomotive, a maritime navigation problem or a forest-river ecology (harmony), one has to consider the importance of some signals and disregard the noise. This is how a thought style makes a difference between groups, as it makes different signal-to-noise ratios and different cross-sections through reality as seen by the lens of particular knowledge. If you can see details like imposed arbitrary characteristics of some choices, personal preference or "human touch", you are looking closer to the thought style.

In contrast, a thought collective is based on social familiarity. Members of your thought collective, or your research sub-field, may not be the members of your laboratory, but you consider them your colleagues. Sociologically speaking, if you can imagine being in their place with only a small change of circumstances, they will be your collective. You may not be specialising in the same sub-field as them, you may be working in a different sector, but at least you do not consider them outsiders or laypeople.

A good example would be two hypothetical colleagues from the university. The first one pursued an academic career in cryptology. The second pursued a

career in a security start-up or in the military. They work in a similar field; they may even have some collaborations or joint publications. Their thought styles may slightly differ and their goals and research differ as well, but a sociological translation would still remain possible. They may not be able to imagine equivalences in detail, but the basic social illusion is good enough to hold a private conversation. They would differ in thought styles, but they should be a part of some thought collective. Not all of their professional jokes or "war stories" would land on one another, but at least some should be mutually intelligible.

This also scales with solitude. Your thought collective is shared with the field, but a thought style is very individual. Even within the laboratory, its members differ in perspectives. Sometimes those result in errors, but on other occasions, thought styles result in discoveries. This is not to say that there are no multi-member experimental teams, of course, there are. This is to say that, even in most coherent teams, each person is looking at their part on their own.

Even in a large team, one may feel terribly alone with one's thought style, at least until some confirmations happen. Even after non-human confirmations, the seed of doubt is often there: Have I made some mistake? Do I have some bias? Have I missed something?

Here comes the most beautiful and, perhaps, the most mischievous paradox in the sociology of science. While you can, at least theoretically, be solitary in your thought style, to confirm anything from your discovery, you need your thought collective. Your home lab is good for the first round of testing, but they are often too close to your thought style. Your close colleagues share your backgrounds, biases, equipment, funding, etc. You need colleagues who know what you are talking about but with enough difference to get a cross-perspective; otherwise, the biases that are associated with social closeness may get into the vat. I believe this makes science or technology so beautifully social and how it transcends humans, cultures and ages. To figure out really complex stuff, you have to triangulate really, really hard. It is also mischievous because it dialectically relates solitary depths of human cognition, their creative process and abstraction with absurdly complex social structures.

This is exactly why I believe it is pointless to argue whether (techno-)scientific discovery is done by a singular person or by the community. As humans, we can decide it only after the science has settled the questions. Until then, the science is what happens between a thought style and a thought collective through the interface of a laboratory.

So, there cannot be any other example for my understanding of the thought collective than the "big one": the set of security vulnerabilities known jointly as Spectre and Meltdown. As with many other examples in this chapter, what could easily have been separate books will be only simplifications invoked for the argument. I am almost surprised that no other philosopher or sociologist of cybersecurity tried to engage intellectually with it, but as the saying goes: "there cannot be elephant in the room that would be too big to be framed out of conversation happening in the same room".[3]

The overview of vulnerabilities is given by a popular paper by Abu-Ghazaleh et al. (2019), while a technical reconstruction can be found in works of Prout et al. (2018). The scale is so immense because what later became known as the Spectre and Meltdown families of vulnerabilities affected vast numbers of systems. In simple terms, the computing processors that propelled the rise of commercial computing for a decade or two were so fast because, in optimising the stacking of incoming instructions, they simplified and predicted. However, by eavesdropping and interfering with the order of such predictions, a third party may have gained access to nigh-all results of the processing operations. In a metaphor that is hopelessly nonexpert, Spectre and Meltdown were something similar to listening live to a person's mind by careful manipulation of oxidation balance between the neurons at the scale of the entire brain. By manipulation on the very edge between forecasting, erasure and logistics of billions of commands, in spaces where digital bits and command lines in assembly language became electrical states in semiconductors, the vulnerability could be exploited.

What was fascinating for me as a sociologist was not the scale of the revealed vulnerability nor the discoveries of whole new families of vulnerabilities. No, for a sociologist, what was absolutely breathtaking was the fact that the papers came from research groups of completely different sociological origins. Wham! Google Security Lab. Wham! University Lab. Wham! A small cybersecurity company. Wham! A collaboration between freelancers and some of the authors of the previously mentioned papers.

That was multiple discovery, as known from the history or philosophy of science, or when several researchers in the field working on separate but interconnected problems find solutions concurring to each other. For a sociologist, this is exciting because it shows that a given scientific group achieved such level of interconnections and coherence that groups of different origins came to the same conclusions. What Kuhn tried to explain by zeitgeist or Gestalt in the case of calculus or Einstein, I understood as a sign of coherence, cognitive reinforcement through digital and physical collaborations and a sign that sociological abstractions are still worth investigating. In a span of few years (from 2016 to 2019), the understanding of commercial processors changed, and what I would argue, the understanding of our world changed with it.

By conceptualising the thought collective, I wish not to diminish the authorship of any person or a team that contributed. I am aware that the Spectre and Meltdown discovery comes back to papers as old as 1995. What I wish to convey is that getting to this level of research sophistication and documenting the scale and complexity of this vulnerability required not only the thought styles of geniuses but also the complexity, coherence and development of the thought collective. Because without the latter, it may have taken years to find connections between discoveries. Yet, in 2025, the scale, consequences or basics of mechanisms of Spectre and Meltdown, complex as they may be, are within the perception of a sociologist.

Of course, the questions about the scale, knowledge and lack of production control should be asked if a vulnerability of similar scale was found in mechanical engineering anywhere else. Most likely, they will not be asked publicly. But at least, there is knowledge.

## Summary. What Makes Political Economy of Knowledge in Cybersecurity?

Through this chapter, I discussed three concepts that are helpful for understanding cybersecurity. The "laboratory" helps with understanding everyday collaborations and cognitive actions. The "profession" describes public recognition, public trust and the degree of autonomy recognised by legal and state institutions. The "thought collective" allows for discussing modalities such as interactions between an inner circle of researchers and an outer circle of practitioners and communicators. I am not the author of those concepts, but my contribution lies in recognising their usability and verification in the context of cybersecurity.

Sociology rarely has spectacular findings. To see Spectre / Meltdown as a sign of coherence of the field and to interpret them through the Fleckian concept may appear trivial when the interpretation is presented. Similarly, it may appear both obvious and inconsequential when insurance against ransomware or malfunctioning locomotives are interpreted as incentives in the development of professional jurisdiction.

I believe that sociological conceptualisations have practical implications. For example, without the notion of the laboratory, I would not be able to understand CTF tournaments as equivalents of the replication of experiments, nor would it be easy to discuss cases of sexism and racism in cybersecurity as compared to similar violence in science in Chapter 6. If one takes the concept of laboratory as proposed before, one may ask: what kind of mistakes are met with laudation, which are kept hidden and which are pushed into matters of personal shame of junior collaborators in the given group? How about the Matilda effect? How about social mechanisms underlying researcher burnout: personal identification with their research, peer pressure of the public image of a high-achieving field and many others?

For me, the most interesting implications of the proposed conceptualisations lie in the questions of political economy. Following a long tradition back to Karl Marx, I believe that technology is an applied, material projection of knowledge on labour. After Matteo Pasquianelli (2023), I understand digital algorithms as shaping and emerging from their datasets rather than taking algorithms as finite, well-defined procedures. In this sense, algorithms, as any technologies in history, shape the world by the same opportunity of application. To know that something was done in this and that condition is more than to simply know that something more can be done in the future.

As Spectre / Meltdown have shown, cybersecurity gatekeeps the very foundation of digital abstraction in almost every digital device. In its most

promising and civic form, it is urgently necessary as a form of fourth estate, to reverse engineer locomotives, algorithms, delivery platforms, intelligence agencies, secret prisons, wiretappings and sociological procedures, to ensure that no violence by a human, ethnicity, capital, state or science will escape the public scrutiny.

However, as I tried to convey, the political economy of cybersecurity comes not only from its usefulness to state or capital nor even from its ability to demarcate digitally mediated infrastructures. If digital algorithms not only analyse but co-shape datasets and societies built on datasets (Pasquinelli, 2023), then cybersecurity is the regime of truth-power.

It disappears, reveals or fragments not only datasets or computers but whole societies, sciences, histories and abstraction possibilities. This is why understanding transnational, seismic changes in its laboratories, profession and thought collective is a task for a sociologist.

If this sounds too serious, just wait until the chapter on computer security e-sports.

## Notes

1 Fair use is the settlement of legal debate that rules what is legal to do with the digital system and what counts as infringement of intellectual property. It may relate to software, a gaming console, a vibrator, an encryption system or an agricultural tractor. As a rule of thumb, the European Union provides a broader understanding of fair use, so hackers and consumers have somewhat more freedom of tinkering, etc. It is closely connected with right to repair and capacity of communities to provide maintenance for infrastructures bought by said communities.
2 This reconstruction is based on public sources only, so I name the authors as they publicly claimed the authorship. As agreed per anonymity, I can neither confirm nor deny that any of the researchers from the Impuls case took part in the research for this book.
3 I invented it. It describes the wonderful ability to mutually reinforce repression of reality through shared social conventions.

# 3 “Inbetweeners.”

## Capture the Flag Tournaments in Cybersecurity. Replication. Labour. Recuperation.

Sustenance of humans and non-humans became dependent on the infrastructure. As social life became more entangled in those dependencies, a large part of science and technology studies (STS) grew to respond for the need of understanding (Bowker & Star, 2008; Star, 1990, 1999). While popular understanding often limited the understanding of infrastructure to only systems comprising material objects, this approach proposed a different perspective, one more attuned to the perspective of social sciences.

Infrastructure was understood through a dialogue on the relations between material networks and human communities of practice, their knowledge and embeddedness in history(Star & Ruhleder, 1996, p. 133). Both theory and method relating to infrastructure have been debated with cognition studies in philosophy (Bateson, 2000) and anthropology (Hutchins, 1996). Perhaps this genealogy caused infrastructure to be theorised in STS and was inextricably linked with understanding practices of care, maintenance and dissent by communities organising around the material networks. In contrast, analysing social epistemologies practised in those communities often considers the materiality of networks to be obvious, granted or (socially) invisible.

Were there any counterproposals or critiques? Recent debates on the “infrastructural turn” (Hesmondhalgh, 2021) reveal some unresolved issues. For example, critique often emphasises that IT overemphasises social studies instead of examining the material underpinnings of power relations (Sandvig, 2013). Second, a strain of critique points out a lack of interest in the debate on the broader political economy of infrastructure(Hesmondhalgh, 2021, p. 13). This problem was due to the scale of infrastructure, as over-focus on the minutiae led to losing the “scale effect” brought by the infrastructure.

I wish to engage in a theoretical discussion of STS using data from an ethnographic study of digital infrastructure. Both the theory of infrastructure and the details of digital infrastructure can be complex. This chapter is less interested in privacy imaginary (Rommetveit & van Dijk, 2022), instead, studying the obscure backbone of such imaginaries. I am less interested in providing a case study of a singular security error as an infrastructural exception. CTFs

DOI: 10.4324/9781003396871-4

often escape straight institutional categorisations, but, nevertheless, they form repeatable patterns occurring alongside digital infrastructure.

Because I am interested in discussing theory using fieldwork, I present my theoretical toolbox and the role of each concept. In the first part, I return to the critique of IT (Hesmondhalgh, 2021; Sandvig, 2013) and theoretical synthesis (Lee & Schmidt, 2018). This narrows the understanding of infrastructure and points to some jarring issues. The discussion also lets me situate my proposal and provide some working concepts. In the second part, I outline the basics of critique and recuperation theory from *A New Spirit of Capitalism* (Boltanski & Chiapello, 2007). This is useful as a rudimentary political economy but also serves as a link with other studies on hackers, digital infrastructure and security. In the third part, I introduce the basic concept of CTF hacking tournaments, showing their connection with the political and economic moguls of the Internet. In the fourth part, I show how CTFs stratify different echelons of hackers. Finally, I discuss a detailed replication of the anomaly in the infrastructure and its theoretical details.

## Recuperation and Infrastructure

The concept of recuperation was introduced by Boltanski and Chiapello (2007) in their book *The New Spirit of Capitalism*. It describes a never-ending process through which capitalism is renewed through its critique. Recuperation was used by Boltanski and Chiapello to explain capture of the critique after the 1968 revolts in France. Later, it was extended to studies of hacking and digital capitalism (Söderberg & Delfanti, 2015).

According to Boltanski and Chiapello (2007), network geometry was crucial in shaping post-World War II visions of a critique of capitalism in France. Earlier generations viewed the workplace as hierarchical and organised under Fordist production models. Post-war managers were influenced by military and information technology, so they emphasised flat, networked structures. In popular mythos, networked structures are more resilient to attack than hierarchies. With resiliency came more freedom for individual expression and more space for individual initiative and growth. Arguments like those changed the popular mindset from which artistic and social critique emerged.

The notion of "recuperation" describes the conditions under which capitalism captures its critique to reinvigorate the productive spirit of capitalism and reshape new regimes of accumulation and exploitation. In this sense, the history of capitalism is the history of critiques and recuperations.

My proposal diverts from Boltanski and Chiapello. Instead of focusing on the "spirit" and seeking causes for dynamics, I ask: What happens with critique and recuperation when they operate as mediated on the scales of digital infrastructures? What are the epistemological consequences for thought collectives?

This differs from other applications of *The New Spirit of Capitalism* in STS. For example, critique-recuperation dynamics have been shown with Facebook/Meta policies in countries throughout Africa (Rider & Murakami Wood, 2019). The growth of the network relied on recuperation and recapture of the critique concerning free speech and digital inequalities.

This shift in understanding marks the transition from macro to more granular-scale resistance in relation to critique and recuperation. It is not surprising that recuperation in relation to hacking differs from Boltanski and Chiapello's proposal (2007). Unlike source theory, hacking studies focus on remnants following the recuperation process and the processes of resistance to it.

While capital captures critique, it still leaves remnants and leftovers as embers for future critiques. Those recuperated embers (of future critiques) are not abstract or limited to the systemic scale but are embedded within the human scales of the resistance. This theoretical reconfiguration is essential in two aspects. First, Maxigas and Söderberg (2022) emphasise the constructive dimensions of hacking, highlighting ownership over tools. This diverges from the popular stereotype of hacking as destruction and comes closer to contemporary hacking studies. The central theoretical outcome of Maxigas and Söderberg lies in the recognition that hacking is a practice of worker resistance in critical workplaces in the digital economy. No less important for this work is their recognition that dialectics of critique and recuperation are, by definition, incomplete. Every political transformation always leaves some residuals, both on the side of critique and recuperation. Every revolution, consumed or triumphant, is, by definition, incomplete. These residuals create biographical histories and experiences and shared knowledge for future shifts. Hacking culture can continually restructure and devise fresh means of resistance and reparation because of the political leftovers present, as per Maxigas and Söderberg (2022).

Interpretation and occurrence of residuals marks the difference between this chapter and the research of my colleagues. Hacking can and should be understood as a practice of labour resistance in the workplace of digital capitalism. Herein, I propose further research to recognise this resistance not only in terms of politics, as imagined by philosophy or the sociology of labour or welfare (Well et al., 2023). I believe that hacking matters because hacking is the political critique and recuperation of infrastructure. Materialised, but always beyond a single time-space. Embedded in a community of practice. Not always destructive or anti-systemic, as elusive dialectics of critique and recuperation itself.

Maxigas and Söderberg (2022) focused on building alternatives to commercial digital infrastructure. However, the focus on independent and positive practices of resistance comes with a hidden cost. Understanding the resistance and recuperation of smaller projects is necessary, but it is not sufficient. Maxigas and Söderberg focused on hacking, understood as practices of

construction. They proposed recuperation and critique for cases of independent hacking projects and their subsequent commercial recuperation. I wish to do the reverse: not to focus on hacker culture on its own, but to follow open hacking events as they are held as liminal to affairs of business and military institutions, in order to learn about these institutions. This why this chapter focuses on the politics of hacking almost at the moment of embedding it into transnational corporate and military interests. The interest is still in infrastructure, the objective still lies in science, and the approach is still sociological. The difference lies in the fact that CTF groups are more ad-hoc based and do not necessarily fulfil the criteria of laboratories. In this sense, CTFs are "inbetweeners", a mixture of cognitive, professional and leisure spaces kept apart from workplaces, but staying in proximity to them.

I do not intend to disprove Maxigas and Söderberg proposals but to provide a dialectical counterpart to their work. Where they studied the resistance and capture of independent critique, I preferred an almost completed recuperation, that is, what remains between oligopolies and powerful institutions of military and digital espionage as a necessary common group for the profession. Where Maxigas and Söderberg study autonomous practices of resistance formed around the construction of separated systems, I focus on destructive practices of collaboration, bound by constant rivalry; where they studied anarchist projects captured by the market, I studied the capitalist enclosure of anarchist-like space and the sporadic acts of individual decisions within it.

To understand this recuperation mechanism and its relation to digital infrastructure, I examined CTF hacking tournaments. Despite the recent professionalisation of the field, they still operate in a semi-independent niche. Enthusiasts could say they still gather to provide a breeding ground for radical hacktivists, providing a long-lasting tradition in the hacking culture. Furthermore, it would be hard not to notice that many military and intelligence agencies use CTFs as recruitment tools (e.g., North Atlantic Treaty Organization CTFs and Government Communications Headquarters CTFs). This growth of semiformal practices in security was overlooked in security studies concerned with hacking, even in areas using STS approaches (Bellanova et al., 2020; Bellanova & de Goede, 2022).

During the last decade, hacking studies have broadened the definitions of hacking to include practices other than those connected with information security (Coleman & Jandrić, 2019; Dunbar-Hester, 2019; Lindtner, 2015). Where my colleagues focused on independent communities and non-security types of hacking, I focused on the practice that is in the middle of recuperation.

## Outline of CTFs

At first glance, CTFs are private or semi-private gaming events hosted and participated in by the community. Only after interviewing the participants, mingling with them and learning more about different interested parties can

one understand their scale and relevance. They are far from enough for statistical generalisations but enough to test a few theoretical concepts.

CTFs events usually take from 12 to 36 hours. They are played during physical or hybrid physical/online meetings. Online CTFs were less popular before the COVID-19 lockdowns. After 2021, there appeared to be a return to on-site events. CTFs are held during various security events. The most typical events happen during security conferences or hacking conventions, but there are also events independent of other security meetings. CTFs are organised by the players themselves. Yesterday's players and competitors become tomorrow's arbiters and task authors.

For a community focused on researching errors and irregularities, proximity with practice may be even more important than for people who "only" develop new solutions. Errors in infrastructure require an infrastructure different from concepts of possible new developments, even on a very direct material level. Ideas and possibilities of infrastructure are much easier to conceptualise in abstraction than in errors.

This difference becomes even more visible when one considers different CTF formats. Teams compete in solving tasks given by the judges (the so-called "Jeopardy" format) or against each other (attack-defence format). The former usually involves more cerebral, focused and extended events. The latter is shorter and more confrontational, as teams simultaneously maintain their infrastructures and attack the IT infrastructures operated by other teams. Points are scored for maintaining a stable service and for disrupting the services of others. In attack-defence events, part of the team must assume the role of defenders and system administrators. Attack-defence hacks often require make-do, "good enough" solutions rather than long-term strategies. This also resembles a popular split in security. The red team focuses on offensive research, and the blue team focuses on defensive research. During "Jeopardy" formats, this logic is shifted. Tasks are not divided into offensive/defensive but into specialisations, as shown in Table 3.1.

Both types emphasise the two elements of a thought collective. Attack-defence is the simulation of attacks on large infrastructure in real time. Methods are often crude, everybody is high on adrenaline, and defenders often resort to using honeypots. Using these, they try to bait the attackers into revealing and disclosing themselves, making hostile actors vulnerable to counterattacks or identification. Jeopardy CTFs are usually longer. Their ebbs and flows relate more to cerebral exhaustion and not to opponent actions. Interviewees described them less as minefields and besieged ramparts and more as puzzles and ornate tapestries.

If attack-defence evokes a real-time emergency or popular representations of military cyberspace operations, "Jeopardy" CTFs are closer to planned anti-infrastructure projects, science or espionage. Attack-defence model situations are like "all hands on deck" where an incident occurs on the network as the team exhausts the recommended caffeine dosage for a small village.

Jeopardy CTFs are slower and more methodical. Problems benefit more from a careful selection of techniques than the "good enough" approach.

Time framing matters not only for understanding social changes but also for understanding political framing. The difference in time framing between different projects was explored in STS a long time ago (Traweek, 1992). It is still relevant in STS research on robotics and space communication (Vertesi, 2015). Despite this, little is known about time framing and the infrastructure and differences in time framing within the thought collective. I cannot discuss this here in more detail. Still, the participants noted and appreciated that the CTFs allowed them to "experience a different rhythm" (from an in-site impromptu interview). It was not only about the condensed, intense, flow-inducing feeling of competitive hacking. For some players, it was precisely the opposite: the CTF tournaments were more cerebral and more reflective than other events in their professional lives.

This split between reflection and hectic action is also mirrored in the two types of games. Attack-defence CTFs are hectic. There is an almost continuous feedback loop between the attacking and defending elements of one team. When defenders identify what is thrown at them, the attackers gain a new tool in their arsenal. Sometimes, the situation resembles war games, as attackers delay releasing a new offensive until defenders prepare to defend against the same method used against inventors. Observing a team playing attack-defence is like observing an emergency command centre. Attack-defence CTFs are like "blitz" chess: exhausting, engaging and demanding ruthless attention.

If attack-defence is "blitz", then "Jeopardy" is classical chess. Everybody around the table speaks in hushed voices, as all other team members are engaged in rigorously complex thinking. When CTF players discuss the possibilities of solving tasks or some properties of electronic systems, it was not uncommon to hear the invocation of theorems, papers and formal proofs. Of course, hacking is much more than the formal sciences, so underground zines, gossip and news from security conferences are also discussed as viable hints.

Teamwork in "Jeopardy" events is less focused on crossing the divide between offensive and defensive hacking. Interviews and casual talks more often mentioned cross-specialisation discussions. More complex tasks often move from one category to another, exercising constant switches between classifications shown in Table 3.1. When interviewed, participants said that this ability to recognise problems from other subfields was a benefit of solving tasks outside their primary specialisation. In this sense, CTFs provide the opportunity to learn details within the subdomains of security. What is even more important, those details were presented as interwoven with each other, so hackers and professionals also learned them in associated contexts.

This richness of interwoven contexts, technical subtexts and deliberate misleads makes CTFs living test beds for security knowledge. In this sense, it resembles a seed bank or a wild habitat. CTFs are numerous, ubiquitous and varied in sophistication and accessibility. They reflect not only changes in

hacking culture but also changes in security epistemic culture. Notice how one participant emphasises the unique and detached character of CTFs in Fragment 3.1. The participant's discussion of temporal separation furthers the idea of "ritual condensations and celebrations of hacking lifeworlds"(Coleman, 2010). Biella Coleman's remarks on rituals in hackerdom almost ideally matched the significance assigned to CTFs by individuals (see Fragment 3.3). The intensity of CTFs is palpable, addictive and contagious. Even with my modest computer security knowledge, I felt energised and compelled to try to understand the solutions. Cerebral festivity is transcribed into a prolonged sense of pleasure from abstract thinking. CTFs are joyful for other hackers, not only because one can see players' actions but also because one may empathise with their state of focus and care.

Each CTF team usually consists of four to twelve players. Depending on the event, there may be rules about the maximum number of players present and their physical attendance. Players share their origins: the same country, company department, or government institution. They self-delegate tasks according to their specialisations (see Table 3.1).

Standards tell stories in STS (Bowker & Star, 2008), but this is even more; this is a meta-standard that serves as a rudimentary categorisation for unknowns. It is unwritten, malleable and held only through social conventions and communal events. It is also a rudimentary, rough and less-than-obvious counterpart for International Classification of Diseases Eleventh Revision (ICD-11) but applicable to errors and anomalies in digital infrastructures. While STS research on ICD often understood it as a layer of the infrastructure of human health (Aue, 2021), its counterpart for digital infrastructures escaped such scrutiny. However, STS should study both, despite the former being more abstract and distant from everyday experience.

Perhaps this is why making systematics is even possible, although absurdly complex. This may also be why there is no finite list of CTF categories, as the list changes and mutates as the hacking itself. Through this incompleteness, CTFs allowed an understanding of digital technologies to be shared, replicated and disagreed upon. This also allowed a continuity of the hacking

> I like the adjacency, the cerebral tension. I like this special character of the event, outside the regular job. I like how events are focused and detached from everyday time. I like the whole setup, just to sit and fuck about with the tasks. (paraphrased from interviews).

*Fragment 3.1* The celebration of the lifeworld of the hacking culture mixes with the joy of cerebral exercise. This cerebral exercise of solving and replicating security problems becomes open to recuperation as unpaid professional training and mental work.

*Table 3.1* Categories of CTFs

*Categories of CTF tasks in the "Jeopardy" format. Changes in the categories of CTF change the information security profession and infrastructure. Reverse engineering is directly recognised as a separate specialisation, on par with cryptography. While cryptography is recognizable as an STS subject (West, 2022) of study, reverse engineering might be more problematic. Hackers were the direct inspiration for the theory, but the history of engineering provided many other examples.*

| *Abbreviation* | *Technical area* |
|---|---|
| Crypto | Software applications of mathematical cryptography. |
| Rev, RevEng | Reverse engineering, or figuring out how closed and unknown systems work. Opening black boxes outside STS, (e.g., in electronic systems). |
| Bin | C programming language and assembler operations on memory. Sometimes, the exploitation of binary files. |
| Web | Using characteristics of web pages, technologies such as HTML, etc. |
| Forensics | Recovering deleted files, parsing through data seeking hidden messages, analysis of patterns in images. |

culture and a continuity in the thought collective despite several eras of technological changes. Following and extending Gallison's model of intercalation in trade zones (2008), one can hypothesise that thought collectives offer anchoring for periods of changes in infrastructures. A reverse relation is also likely to be true, as turbulent eras in thought collectives are anchored and stabilised by the materiality of infrastructures.

Observing CTFs shows that dialectics of error and repair by infrastructures mirror dialectics of critique and recuperation in a thought collective. Cycles of errors and repair in the infrastructure could even detach themselves from the time-frame of public politics or cycles of public interest. If the infrastructure is overlooked as obvious when it works, then errors in the infrastructure could be doubly invisible for public and non-involved actors.

Now, it is time for the next step. I mentioned that the thought collective is stratified, depending on the level of abstraction and gatekeeping of knowledge. Now, I offer an overview of such processes in thought collectives.

## Communities and Crowds: Stratification of Thought Collectives

CTF events vary in participant numbers. The most significant events exceeded 400 players. The smallest ones may have only 3 teams and 15 players. What makes the difference is not the number but the professional composition of the participants and the relative prestige of the event.

During critical events, I had the opportunity to talk with the profession's elites. They included senior specialists from the security departments of 10 highly visible software companies, academic cryptographers, security researchers, highly paid penetration testers and security architecture

consultants. Perhaps less known to the public eye, but no less critical, were national Computer Emergency Response Team (CERT) specialists. CERTs are like national surgeons or consultants of medicine for emergency response in security emergencies to those outside the field. For reasons of anonymity and duty of professional care, I cannot disclose what nations (CERTs), companies, universities or events I have worked with. By design, I did not record names, names of tournaments or dates. Anonymity and confidentiality were important. For top teams, CTF events are arenas for professional prestige, exchanging knowledge and discovering a shared understanding of otherwise under-discussed details. Higher echelons of CTFs are for exchanging ideas, gossip and arcane, tacit knowledge.

CTF events often invoke images of underground, weird or off-putting elements. They serve several purposes. First, they deter interest from people without sufficient immersion in the hacking culture, also serving as an unspoken, elite gatekeeping mechanism. Second, obnoxious and confusing symbolism adds to participants' cognitive and emotive experiences. The cognitive load of technical problems becomes less overwhelming when some elements can be navigated through familiar symbols. Finally, loud symbolism demarcates CTFs as non-work situations. In this respect, CTF tasks mirror CTF aesthetics, as shown in Fragment 3.1.

This set of preferences is both epistemic and cultural. In agreement with Maxigas and Söderberg (2022), I also understand CTF communities as "communities of peer producers". I wish to put forward the observation that the peer-to-peer mechanism becomes critical when epistemology focuses on errors and anomalies.

Players in more prestigious CTF tournaments often use them as attempts to "break into" the elite sectors of security. Hackers and security professionals from this group had the highest labour autonomy and professional expertise, so sometimes they are envied not necessarily for reasons of money or prestige, but because for the opportunity to work "on the interesting problems" (Table 3.2 shows some fragments on this disposition). CTF tasks are like "solving beautiful mathematical problems, a source of bliss and aesthetic sensibilities" (direct quotation from a respondent). Their craft and their practice in CTF matter for infrastructure, because they produce and reproduce gaps, errors, and extreme cases. In my assessment, CTF epistemically serves more for replication, communal discussion, or peer review and less for discovery.

It is a common belief that security departments and other desirable employers observe more prestigious tournaments. Playing CTF is participation in security discourse. Task authors propose critiques of existing technologies. Players recuperate or counter them. Players are proposing security models for various black boxes.

This is the most direct political reading of CTFs. They are political simply because they gather computer security elites at the global scale. Effects of the gathering may vary, but the mere fact of the informally institutionalised gathering at the global transnational and trans-corporate scale makes them

| | |
|---|---|
| *Author:* | What makes a good CTF task? |
| *Participant A:* | A CTF task is good when it brings something new. It is not repeating something that has been done many times. A good task should not be simply tedious or complicated in a way that requires many hours to parse. A good task is a playable one. |
| *Participant B:* | It is very easy to construct a hard CTF problem doing some huge and messed up binary file. Everybody will be reading millions of lines of code for 48 hours and will be none the wiser. |
| *Participant C:* | A good problem should be slightly beyond your current limits. It should also be slightly beyond expectations. |
| *Participant D:* | Bad problems require a lot of blind guessing or pure intuition. A good task leaves breadcrumbs and clues and characteristics akin to real-life slightly unsafe systems. |

*Fragment 3.2* Answers to a question "What makes a good CTF task?" Participants emphasised new knowledge, subversion of expectations and cerebral challenge. Randomness and tediousness are criticised. Observe also how participants emphasise the "good kind of broken system" from the bad one. This is akin to the expressions of epistemic aesthetics' recognition of mathematical proofs.

political. Whether they function more as knowledge exchanges, professional leisure time or recruitment events should be investigated in detail in further studies.

Now, I discuss a less glamorous part of the CTF scene. Colleagues from less prestigious or more local events are more likely to be at the beginning of their careers. Some may be students or software developers in transition to security. For others, local CTFs may be a pleasant change in the routine of an older academic network administrator or a local Linux guru. Some may be artists "just dipping into the sec" (direct quotation) or other types of occasional aficionados. An example of such a CTF can be found in Fragment 3.2.

Maxigas and Söderberg's (2008) typology recognises this group as "crowds of users/audiences". They are above the level of "click workers", as they still have significant autonomy and expertise. Their CTFs go beyond just replicating tasks from more prominent events. For example, tasks may require brief familiarity with Shodan,[1] a dedicated search engine for the Internet of Everything (IoE). Such search engines have applications in security, so Shodan tasks are often proposed, and Shodan individual subscriptions function as popular prizes.

> IrisCTF is a 48-hour Capture the Flag competition organised by IrisSec. IrisCTF takes place the first full Friday-to-Sunday weekend every year online and features challenges in the disciplines of reverse engineering, binary exploitation, web exploitation, cryptography, radio frequency, networks, forensics and more. IrisCTF is meant to be, above all else, a fun, light-hearted and educational experience for all.

*Fragment 3.3* Organiser's description of the CTF. I identify this event as a "crowd of users/audiences" event. It emphasises lightness, a welcoming character and education. It also visibly demarcates the specialisation of expected tasks.

While the framing of a "crowd of users" easily applies to local events, the category of "audience" is less applicable. During "crowd" CTFs, blurring the boundary between the audience and participants is even more common. They are communal not in the sense of global security experts' community but in the sense of local communities of security specialists and administrators.

This is the second aspect of the politics of infrastructures and thought collectives. CTFs serve as peer mediation mechanisms and knowledge-sharing rituals between different digital security approaches. If "peer production" CTFs are more similar to critique-recuperation dynamics at the transnational scale, then "crowd" CTFs resemble a controversy about cracks in a newly built local pedestrian bridge.

Observing communities involved at different levels of the thought collective provided some findings about the politics of infrastructures. As in IT, knowledge about infrastructure is often circulated through communities of practice. What may be surprising is that communal events and knowledge rituals are still valued, even for highly distributed and remote digital infrastructures on all levels. This is the most "social" aspect of the politics of CTF, simply an act of being together with other practitioners from the otherwise elite and often secluded profession.

The next layer of politics is built atop social gatherings. CTFs have become political recruitment and propaganda tools. Notice how valuable the gamification is in this case. It allows us to play around security and hacking without conflict with the secrecy of the workplace and "serious" infrastructure outside of a CTF. In this sense, the space-time reduction of seriousness and "serious politics of serious infrastructure" makes them political.

Labour resistance is another dimension of labour relations (Söderberg & Maxigas, 2022). If one considers hacking as labour resistance of skilled labour elites, how does unpaid CTF play-work or play-education fit into this logic? Throughout the history of technology, craftworkers insisted on payment for training because of a belief that work should be paid for (Kaiser, 2005). From

this perspective, the non-direct benefits of otherwise unpaid CTFs become political, similar to open science (Mirowski, 2018). This applies to the arena of critique of existing knowledge/power relations and the process of recuperation of knowledge shared in the community without payment for the sustenance of the community.

## "Hack Me Baby One More Time": Replication of a Security Exploit

In previous sections, I discussed the conceptual, political and social ecologies of infrastructures. In this section, I discuss the replication of the anomaly, its materiality and its politics.

For the sake of privacy, I anonymised and generalised technical details and reconstructed a biography of a generalised task. For the sake of simplicity, I discuss only tasks from "Jeopardy" CTFs, as they are easier to transfer between the events. However, because the process may appear convoluted, a summary is included in Table 3.2. Notice that my reconstruction goes beyond a singular CTF event as it includes the pre-event and post-event life of the task.

As the task authors recollected in the interviews, the process starts with "the idea of a cool problem". Usually, this is a gap in the digital infrastructure or a security exploit. The author repackages it into a different context. Old problems re-emerge in new versions of systems or descendants of old architectures. Analogies or generalisations of security loopholes are created. The task authors reported a solitary process in this phase, although they emphasised communal sources of knowledge and the importance of social knowledge sharing.

It is worth noting that almost no interviewees discussed task ideas in abstraction. They are always related to a particular family of infrastructure or software. Tasks could have been about the generalisation of an anomaly on another class of networks. Still, the idea of the task was reported in relation to the materiality of the infrastructure. Using interview fragments, writeups, chat logs and recorded fresh talks, I reconstructed how security vulnerabilities are abstracted into and from CTF tasks in Table 3.1. This cognitive process is made as a game, which sustained the cognitive engagement through the emotional involvement of the players and teams.

Emotional justifications behind task-making differed. Knowledge-sharing and prank-making were important but so were phrases like "It looked like an interesting paradox. I wondered if people recognise it". I interpreted and empathised with feelings of pride and satisfaction from fragments on clever tasks and mechanisms similar to "impostor syndrome" from phrases on faulty tasks. While many previous STS studies on infrastructure focused on anomalies and their political resolution, less attention was paid to reverse engineering and replicating the cognition of anomalies in the community.

*Table 3.2* Recuperation of critique of the infrastructure – the CTF task model

| | *Phase* | *What happens with the task?* | *The relevance of recuperation to infrastructure* |
|---|---|---|---|
| 1 | Task Idea | The possible infrastructure gap is not yet materialised into the task infrastructure by the author. | The research and conceptual work are conducted. The task author decides what elements of infrastructural critique/hacking will be adequate for the tournament players, tournament level and task category. |
| 2 | Task Preparation | The infrastructure gap is materialised into the task by the author. | The critique is recuperated to the temporary infrastructure of the task. |
| 3 | Task Testing | The relation between the task and the gap is solidified, tested and tempered by the author of the task, arbiters and testers. This happens before the CTF event. | During this step, the critique becomes specialised and encultured into security epistemology. |
| 4 | Task Reveal and Recognition | This task is revealed to the players in the form of test bed infrastructure. The infrastructure gap is hidden and ready to be hacked. | The second step of recuperation. The task is presented to communities and crowds to discover the infrastructure gaps hidden in tasks. |
| 5 | Solving the Tasks | CTF players attempt to solve the tasks. They try to uncover infrastructure gaps hidden in tasks and use them to score points. | This step is a practical equivalent of peer review of the first step of recuperation. It also serves as a science and technology communication mechanism through which communities/crowds distribute knowledge. This is also the most ritualistic part of the event due to its intensity. |
| 6 | Scoring the Tasks | Arbiters confirm mechanisms used and gaps found in the tasks, officially acknowledging scores. | Completion of recuperation through the tournament. Closing of the ritual. |
| 7 | Publishing Tasks and Solutions | Secondary effect. Some players publish their solutions on the web pages of their teams. | The recuperation effect is spread through the role of CTFs in hacking culture and the information security profession. |

In this close-up, one may notice that an anomaly, bug or exploit becomes a treasured and common good. It relies on unspoken, shared trust in the thought collective. Because of this, the act of sharing the anomaly is the act of demarcating the thought collective, constituting one of its fundamental political dimensions. One may argue that, in the age of open knowledge, this kind of tacit communal knowledge becomes even more critical (Collins, 2013).

In the second phase, gaps or exploits gain new, although temporary, infrastructure. The authors of tasks create fictional networks, banks or programs. They are the rudimentary usable infrastructure, or what I call the test bed, for fundamental gaps and exploits. Critique has not yet been replicated and transferred into new systems, although it has already been taken from its original context. During this phase, new politics or themes around the exploits may be constructed.

It may be just a cognitive and material equivalent of sleight of hand, but political choice also comes with it. The task author either chooses to pass on the original context of the anomaly or strips it out of it. The rudimentary micro-infrastructure of the task is sufficient to cover this switcheroo. The decision to depoliticise mediation becomes useful in politics, especially when one wishes to recuperate[2] some less-than-legal hacking practices.

The third phase does not happen in all tournaments but is a point of pride for the most prestigious ones. After constructing them, the tasks can be tested. This is the equivalent of trials done "inside the laboratory" before a paper is published. The task author, organisers of the CTF event and their colleagues test whether the task is "broken in the right way" (as in Fragment 3.2). The task author's judgment gains team approval. In an almost elusive fashion, the task slowly becomes associated with the author, arbiters, tournament and CTF scene.

The fourth phase is the most terrifying. This would be the grand reveal if the task authors used sleight of hand. Tasks are handed to CTF players. The gaps and exploits are still concealed. Only a rudimentary micro-infrastructure is accessible, such as a barely functional mouse port or network protocol that works so slow that it appears almost non-functional. Players could only hope that they would eventually discover hidden gaps and exploits. The event clock starts ticking. The hacking begins, usually to the sound of some utterly obnoxious techno and no less obnoxious anime projections.

The fifth phase is the CTF proper, as I described before. Players hack and consult with each other. Exploits and gaps are filtered from the chaff of the task's rudimentary infrastructure. Arbiters and task authors verify their intuitions about crowds and communities. Through this process, the thought collective forms again. Rhythms of exhaustion and cerebral celebrations occur.

What is happening politically? This is a debate about anomalies and tasks, and task authors and their interpretations. This debate may end up in critique or recuperation, but what matters is that infrastructure and infrastructures

may have one dialogue (between materialities, bytes, and processing powers). Symmetrically, there may be an another dialogue, indirect and mediated through the medium of playing with the infrastructure between the task author and the players, or between the authors of the infrastructure (in the form of manuals or direct calls) and the players. Exclusion from this debate is exclusion from the politics of digital infrastructure.

For example, recent STS studies of hacking have asked why hacking imaginaries rarely question users' disposition in constructing the "deficient user" (Klimburg-Witjes & Wentland, 2021). My empirical answer is simple: important security specialists learn from CTFs, and CTFs do not generally bother with the inclusion of the users. The results are understandable if self-education emphasises puzzles over people using things in engineering. If you do not believe me, try to find a CTF with tasks on the social aspects of computer security. There are less than 5–10% per year, which I confirmed.

Scoring of the tasks is the sixth phase. Arbiters confirm the solutions given by players. The authors of tasks receive congratulations or condemnations. Exploits, gaps and their abuses are recognised. Participants talk with each other during the afterparty. Politics lies mostly in symbolism and handshakes. An exploit or a security gap was replicated, normalised and understood by a wider group.

The seventh phase is also not mandatory but serves as an extra dose of adrenaline and prestige. CTF participants and authors publish tasks and their solutions – discussions after CTF emerge. The first form of discussions is typical of sporting events. They focus on wins, scores, etc. The second form focuses on the details of the task solutions. They act as a second wave of peer reviews for a wider community of security. I believe that recuperation is almost complete at this moment, as the original critique was subsumed into distributed, unrecognisable forms. They could be useful for further critiques but may also be useful for further accumulation.

What happened during these phases? Knowledge of security gaps or exploits were transferred to a broader group. During each step, a mutual understanding of the relationship between the gap and infrastructure was negotiated and confirmed. In the end, what may have been a political critique at the beginning became communal knowledge. It is not as depoliticised but reframed as related to CTF, "just innocent play", etc. Not all gaps and exploits used in CTFs start as radical political hacks, but the chain functions for enough of them.

## Summary

The previous section followed the minutiae of the process and politics of replicating a computer security exploit through computer security tournaments. The whole process dialectically re-sets both infrastructure and the thought collective. The former is changed by the shaping of new tools, new standards and, perhaps, changes in the ontology of potential vulnerabilities. The latter is shaped by

new social knowledge, new personal connections and new emotional meanings around hacking. I gave examples of small political decisions made at each step.

In conclusion, I return to the larger picture. On the macro-scale of transnational infrastructure, CTFs restructure politics and economics in a multitude of ways. As the need for information security specialists rises, CTFs are still essential to the self-education and self-identification of security specialists with the hacking culture. This may be read as gamification of the hacking culture by corporate and military actors and understood as an example of recuperation and depoliticisation. At the same time, this also means that information security has become more accessible and inclusive. If hacking practices described by Maxigas and Söderberg could be considered workers' resistance, then CTFs could be interpreted as gamified and inconspicuous strike-breaking mixed with widening the workforce through education and unpaid affective labour.

However, I believe that the politics of exploits reach much farther, both in materialised and social form. I outlined only the implications of seemingly neutral trading zones (Gorman, 2010) for security studies. From the historical studies of laboratories in electronics (Galison, 1997), it is recognised that the research time-space "in-between" of institutions may gain political dimensions not despite but precisely because of apparent neutrality. Moments such as perhaps illusory depoliticisation during the replication of an exploit to the temporary infrastructures look like the perfect equivalent of such trade in the scale of the individual, singular exploit. The infrastructures played through CTFs are not "real", they are only equivalents of terrains and props for the game. This particular gamification removes political and moral stakes and allows to examine exploits as "pure, objective problems". This makes CTFs a very special examples and instances of social structures equivalent to the laboratories discussed in Chapter 2. Reframing politics through gamification comes symmetrical with laboratory demarcation. What was invoked for the purpose of the game, leads to very tangible material-digital reconfigurations of the infrastructure, not because the play changed infrastructure per se, but because it changed socio-political relations, which reconstituted a new arrangement of infrastructural vulnerabilities.

How do such reconfigurations matter for more significant shifts at the scale of transnational processes and political economies?

Is it hard to conceive that at least some digital infrastructures cannot stagnate technically and economically because of CTFs? Would it be enough to sustain at least some of the dialectics of critique and recuperation of surveillance capitalism (Zuboff, 2020), even though the initial catalysing spark of "Californian Ideology" took place in the 1990s (Barbrook & Cameron, 1996)? In this chapter, I have provided arguments for at least stating such questions in the STS debate. The CTFs are the dialectical paradox: they are the socio-epistemological stabilisation for replication of instabilities in the digital infrastructures. They serve social and epistemic functions of laboratories,

blending advanced, vocational, "lab bench" training with the function of replicating the knowledge. It is through CTFs that institutions of cybersecurity have some common understanding of the field, without the need for exchanging business, legal or any official communications.

Due to their obscurity, CTFs are easy to discard as irrelevant minutiae or as "just a leisure activity for the field", with little relevance to moguls like Google or concepts as broad as techno-feudalism (Varoufakis, 2023). They are far from the user's perspective or even the perspective of a singular controversy over digital infrastructure. CTFs matter because they are available for every digital system. Every dimension of digital infrastructures was analysed through the games, from digital aspects of water infrastructure through satellites to IT used in industry. CTFs matter because they are infrastructure over digital infrastructure. Over 10,000 CTFs are played yearly, with more than 30 teams and more than 200 players playing major events. This is the scale of quantitative scientometrics.

The sheer scale of computer infrastructure passed through the CTF tournaments elevates exploit replication to the scale of political economy. If participants decide to share an exploit for free on a CTF, rather than selling it or keeping it secret, this is a significant politics of knowledge. It is obscured from everyday knowledge (Voß et al., 2022), and even economic sciences rarely consider exploits as economic goods. Yet, the simple fact of CTF games, their accessibility and barriers constitute the hidden politics of digital infrastructures. STS, hacking and security studies should be conducted on par with digital infrastructures. Perhaps there is no better scope into the details of otherwise hidden minutiae of digital security. Computer security provides a unique opportunity to assess global social epistemology in digital infrastructures.

In 1933, Ludwik Fleck noted, "There is no scientific cognition that is not a cultural cognition". If so, then social processes like CTFs should be understood if not as science of computer security in a narrow sense, then as practices that at least share some social functions with science, as exemplified in Chapter 2.

What Maxigas and Soderberg called recuperation is basically a way of freeloading of employers on researchers' passion in their craft. This is also mirrored in critical theorising in sociology of science: countless hours spent in laboratory witnessed and marvelled by ethnographers of the laboratory, such as Fleck, Latour, Knorr-Cetina, Collins, Larmont, Wagner and many others I still find inspirational for this book, my generation theorise also as self-exploitation. As I interviewed one post-burnout devop and a security researcher: "Passion, emotions, curiosity, cognitive fever, all-nighters, beauty of the puzzle, high stakes of covered problems, camaraderie, prestige or rivalry are great but in the end of the day count your work hours and look at the payslip". I cannot confirm nor deny that this interviewee is currently writing their comments on Das Capital.

I agree with Maxigas and Soderberg about using the framework of recuperation, because in the context of cybersecurity it is about changing infrastructures and datafication attempts vital for lives and labours of the others. CTFs should not be interpreted as simple machinations of capital, vampirically poaching over hacking culture and bleeding its dry. No, in this metaphor, the connection with informal, rebellious and even much more politicized hacking is left as interface for institutions, as a way of sharing recruitment pool and as a source for individual non-monetary motivation.

## Notes

1 It is no surprise that the name Shodan originally comes from the 1994 computer cyberpunk game "System Shock". In this title, Shodan was maleficent AI involved in a technology-mediated BDSM parasexual relation with the hacker-protagonist. Also, Shodan wanted to destroy the world.

2 In thermodynamics, recuperation is associated with reuse of waste heat. Maxigas and Söderberg (Söderberg & Maxigas, 2022) adapted this concept from Boltanski and Chiapello's "New Spirit of Capitalism" (Boltanski & Chiapello, 2007) as a part of dialectical model of hacking. For Maxigas and Söderberg, recuperation meant the process through which proposals alternative and critical for digital capitalism become adapted as new market innovation models, new ideologies for labour exploitation and new ways of disempowering future's criticism of capitalism. What Söderberg and Maxigas defined as a dialectical rest, the remaining that resist to be recuperated in the given cycle, is very close to my understanding of Czochralski's residue from the beginning.

# 4 “Normal Science.”

## Cybersecurity as a Science. Stabilised Instability. Systematics. Power Elite.

In previous chapters, I described various sociological elements of science. In Chapter 1, I described the relation between knowledge, the migration of the workforce, formal and informal knowledge spaces and infrastructures associated with them. In Chapter 2, I described the cognitive characteristics that may be shared more often around the researchers’ in-group than in the out-group. I also described the basic model of a security laboratory as a general type, which includes interfaces with other social institutions. This enables us to identify prestige-reference mechanisms and makes it easier to discuss issues of error, discovery and originality.

In this chapter, I wish to discuss how cybersecurity systematises knowledge. In the previous chapter, I discussed how relatively simple elements of computer security knowledge are replicated in CTF tournaments. Now, I will describe both simpler and more complex discoveries of computer security as objects I call “stabilised instabilities”. In the previous chapter, “stabilised instability” could be applied to knowledge passed between people through personal, informal, tacit, in-situ and trans-institutional circumstances such as Capture the Flag tournaments. Here, I am interested in cybersecurity knowledge that is passed indirectly, without personal contact, often with mediation of the text, code or systematics, in ways that are codified by institutions or, at least, by intersubjective design.

The previous chapter was about cybersecurity that happens face to face, through subjectivities of elite circles or details that happen in the peripheral vision. This chapter is about cybersecurity that happens on the scales of systematics, patterns and databases.

Before discussing those systematics, patterns and cases of their application, I need to prepare my theoretical tools. Digital systems can be broken in so many ways that I need an interim concept that will be understandable both for readers from technical fields and from social sciences. This is why I wish to think through the concept of stabilised instability; I hope it is theoretical enough for my colleagues in the sociology of science while remaining close enough to practical applications for readers in the field.

DOI: 10.4324/9781003396871-5

## What Is Researched by Cybersecurity? Stabilised Instability

In the previous chapter, I described instability as a hackable, breakable pattern. This pattern is breakable in an exact, semi-stable way, and, as such, replicating or using the break is akin to when virologists replicate or splice strains of viruses. The system in which the stabilised instability is hosted is important only as much as it allows for characterisation of the particularities of the stabilised instability. If the particularities of data architecture (e.g., hotel list, Cayman Islands offshore accounts, emails, photos, DNA data, lost books of Plato, datasets, the plans of a latest weapon, an NSDAP photo of Martin Heidegger) are not important, they play an insignificant role as the brand of beads in a virological paper. They become mentionable only when replication goes wrong or when the instability is forked into differently operating variants.

What is "stabilised instability" in the context of cybersecurity? It is any sufficiently intersubjectively exchangeable fragment of knowledge about digital infrastructures that allows cybersecurity researchers to understand, interpret, locate or attribute situations or moments related to weaknesses in the architecture of digital infrastructures or human errors of their maintenance, operation or use. Stabilised instability must be understood in the scope of a thought collective of some cybersecurity researchers without directly correlating interests, as some social equivalent of philosophical objectivity.

On the philosophical side of things, stabilised instability is defined as an epistemological tool and a product of instrumental reading of the science of cybersecurity. Instrumental in this context does not mean that cybersecurity necessarily serves some nefarious purposes. In the philosophy of science, instrumentalism means that science provides models for successful operations in the world rather than general laws about reality. As such, instrumentalism is connected with the philosophical traditions of anti-realism and the writings of Nancy Cartwright (Cartwright, 1983) or Ian Hacking (Hacking, 2001) more than the concept of falsification, perhaps more popular in media and in science communication, introduced by Carl Popper (Popper, 2010).

Grounding "stabilised instability" in instrumentalism makes sense not only in the context of sociology of science and connections of my thinking to ethnographies of Harry Collins (Collins, 2019) and their reception in the philosophy of instrumentalism (Cartwright, 1991) but also to recent and ongoing debates in the philosophy of science focused exactly on the issues of cybersecurity conducted by Jonathan M. Spring, Phyllis Illari, David Pym and others (Spring et al., 2017; Spring & Illari, 2019, 2025). Both Collins, as an ethnographer, and Spring and co-authors, as philosophers, engaged with the works of Peter Galison on the history of particle physics, the radar laboratory and the cybernetics of Norbert Wiener (Galison, 1994, 1997, 2010). Such works will also be an important point of reference, as they all engaged in previous debates on the issues of formation of new scientific fields, their

philosophical and sociological mechanisms and particular issues connected with experiments, simulations, objectivity, methodology connected with late 20th century digital research.

Why is instrumentalism important for "stabilised instability" and for cybersecurity, in particular? Why am I not satisfied with the notions of "text", "performative" or even "inscription"? Maybe I could just dig up some tool from the prehistory of my own field, from the old times when social studies of science appeared to be in dialogue with cognitive anthropology (Latour, 2012)?

Yes and no. Stabilised instability has some traits of a text, or a performative or an inscription. It is stabilised and intersubjectively transferable, like a text. It is scalable, like data in physics or biology, and can be recomposed in diagrams, maps, schematics – cybersecurity uses those, especially in tools such as Ghidra or IDA for analysis of malicious software. It is understood that digital infrastructures move between scales of numbers in places that defy anthropogenic logic. This makes cybersecurity so hard to learn at the level of the individual and even harder to convey at the intersubjective level. This also makes particularly important the fact of stability: without careful documentation, without reference to the infrastructure, its failures and effects, the vulnerability will disappear and cease to be recognised. It will not exist outside the context of a personal meeting of two specialists, like an elaborate professional dance or the scientific equivalent of an artistic impression.

Yet, stabilised instabilities are traded in black markets (Georgoulias et al., 2023). They are also estimated, forecasted and financialised into insurance assets (Edwards et al., 2019) connected with actuarial models related to cybersecurity. Stabilised instabilities spread through digital infrastructures as knowledge objects, but, equally important, the need for them spreads as digital infrastructures expands. Finally, as I have shown in the previous chapter on Capture the Flag tournaments, stabilised instability includes matters of professional prestige, tacit knowledge and individual meaning. While some of those descriptions can be applied to the category of texts, not all texts will carry those properties in relation with the specific professional group or knowledge field. For this reason, I am not keen to understand stabilised instabilities such as texts or inscriptions, even though studies of both categories certainly contributed to my understanding and may certainly be valid for future research.

Instead, I conceptualise stabilised instabilities as performative anti-structures,[1] which is a concept I took and modified from the anthropological research of Victor Turner (Turner, 1995, 2008). In doing so, I think of epistemological objects in cybersecurity less as stable objects, like replicable experimental protocols in particle physics or immortalised cell lines like HeLa (Knorr-Cetina, 1999), and more as combinations of instruments, data and circumstances that contextualise as instabilities are put into action.

It should not be surprising that as a sociologist, I do not subscribe to such divisions. There is no knowledge nor science, on any significant social or

institutional scale, without issues of social order, gender, politics, economy, sexuality and various other dimensions of power. I already discussed how Capture the Flags are examples of embedding with personal and cultural meanings, which are then recuperated as unpaid labour by companies and military institutions. This labour is scientific labour in a very specific sense, as Capture the Flags (CTFs) provide value not only to players by status-marking or to employers by reducing costs of training by gamification but to capital in general by reducing transactional costs by replicating knowledge in the field. This is why CTFs are sites of replication, standardisation and recuperation of stabilised instabilities. This is also why, in my conceptual framework, there is no difference between knowledge, anti-structure and socio-political consequences.

Stabilised instabilities are performed, which means that they can be transferred as they are enacted with corresponding infrastructures. Instabilities can exist in a theoretical sense as abstracts, but understanding vulnerability without a practical example is much harder, as with viruses. This is why standardised reference points, like standardised weaknesses or vectors of attack, matter so much, both in virology and in cybersecurity.

As a sociologist, I am interested in the social function of epistemic objects. If stabilised instabilities are circulated and contribute to the shaping of security knowledge, they also change some social relations. Some of those changes happen within the in-group of the cybersecurity profession or within the field of cybersecurity science. Others happen on the outside or at the intersection with other groups, on broader scales, through the mediation of digital infrastructures in government systems, healthcare, private lives, commercial services or activities connected with surveillance, policing, border demarcation and incarceration. Organising a private, invitation-only security event may be an example of the former, while announcing a new cybersecurity awareness campaign may be a sign of the latter.

What matters is the fact that stabilised instabilities often restructure digital infrastructures at scale (this is how I defined them, and this is how the profession defines them, as I will show later in this chapter). As I discussed in Chapter 1, for a sociologist of science, infrastructures, including digital ones, are not simply instances of locally accessible interface points like computers connected to the Internet. They are neither reducible to abstract maps nor even standardisation systems (Lampland & Star, 2009) that are used to systematically construct scalable maps, ontological and symbolic frames or poetics (Henke & Sims, 2020; Larkin, 2013; Star, 1999; Star & Ruhleder, 1996).

I read infrastructure theory by Star and co-authors as a sociologist, so, for me, the infrastructure is a social image, almost a Durkheimian totem (Durkheim, 2008). In a way, the infrastructure is not only a representation but also a metaphorical social heart of a community that cares about it. This heart often turns to become invisible, misused, overhyped or taken for granted until it fails. When it fails in multiple sites and on a scale larger than incidental, the

failure is not only an issue of a technical, but of a social and political, crisis. This is how infrastructural labour is inextricably connected with a community of practice, often an unspoken set of rules and procedures of maintenance and replacement. This is important both on a socio-anthropological and on a psychological level.

The socio-anthropological one is pivotal for understanding the science of cybersecurity, but before that, I must make a small digression for the psychological one.

What I constructed as a hyperbole, or a weberian ideal type,[2] has actual and harmful consequences for people in the field. It leads both to self-harm through over-attachment and through exclusionary practices. It happens because if the field of research becomes a matter of identity, then people of different ethnicity, gender, sexuality may be individually or socially experienced as danger to this sense of self. From the very onset of research in hacking and cybersecurity knowledge in the 1980s among American self-educated hackers, it is known that learning and experimenting with cybersecurity may be connected with the sense of self (Turkle, 2019). It is not a population-representative study but an interpretative one. It also is biased for one country and a middle-class, white and educated demographic, and times and technologies have changed massively, but I would still use it as conjecture.

As I discussed in ethnographical accounts in Chapter 1, beginners in security or in server maintenance often are over-attached to infrastructures they maintain, so the self-identification often leads to burnout. In the sociology of labour or technology, it was observed in the 1990s (Orr, 1996) among maintenance technicians responsible for Xerox machines as well as among mechanics engineers (Bucciarelli, 1996). Lately, it was a cause of strife between maintenance engineers and science teams working with synchrotrons (Doing, 2009) and planetary rovers (Vertesi, 2015). Recent studies recognised that stress among cybersecurity professionals that report vulnerabilities may lead to burnouts (Moura & Heidemann, 2023).

While I have only proximal familiarity with psychological and therapeutic interventions, I wish to put forward a hypothesis: stress and burnout among cybersecurity professionals is two-pronged. The first element relates to self-attachment to the social and material practices of infrastructure; they experience stress because they personally feel that they are breaching the social norm. The second element relates to a sense of self related to their work, so this may be a semi-conscious connection between doing security, maintenance or care work and feeling smart, capable or careful. While this hypothesis was not verified for cybersecurity defence, maintenance and research professionals, the evidence from burnout studies for doctors, nurses and other health and biochemical researchers that have contact with patients suggests that occupational burnouts often differentiate even in similar institutions (Messias et al., 2019). This digression is already too long to discuss the issue of burnout in scientific careers in length, but I wish to add that in the field of physics (much more coherent and better understood as compared

to cybersecurity!), the trajectories and burnouts as seen through longitudinal studies in previous generations also differentiate, more due to emotional workload than to initial conditions (Hermanowicz, 2009).

Why was this psychological digression important? Because even if my hypothesis is not necessarily true for a significant group size, the psychological mechanisms of attachment and transverse between the self and the infrastructure provide interpretations on why debates on stabilised instabilities often take the form of public performatives.

Conceptualising stabilised instabilities as performatives, I indirectly refer to a concept by Bruce Schneier, a renowned cryptologist and cybersecurity expert. Schneier coined a phrase "security theatre" (Schneier, 2009) to describe actions that are performed to instil the sense of security among the public, but they do not actively improve it. Security theatre in this way was performed to improve trust or respect to authorities or to make them appear as if they are acting.

This is, however, not sufficient for my understanding. Stabilised instability does not have to be publicly understood or even publicly known to make changes in infrastructures. Yet, the public, at least the global Anglosphere and some of its translations into other languages, is still fascinated by the hacker, as a socio-cultural prefiguration of the wise-mage. This is self-reflection, as drawn by cybersecurity researchers who theorise about their cultural representations (Adams et al., 2020). One can ironise about representation or about culture theory all day long, but the sociological questions persists: Why are security professionals understood through those archetypes by the public, and what consequences does it have for the public understanding of stabilised instabilities, as a particular subtype of public understanding of science? The social fact does not stop mattering as a question of research only because it is silly.

The first clue was shown by Steven Shapin and Simon Schaffer in the 1980s as they examined the history of public experiments with vacuum pumps as conducted by Robert Boyle in the 17th century (Shapin & Schaffer, 1985). Contrary to the version given in popular histories of physics, empirical evidence and experiments were painfully slow in changing scientific consensus. Boyle's experiments were always a step behind theoretical critiques developed by Thomas Hobbes, acclaimed as author of the political treatise *Leviathan* and a statesperson. As Shapin and Schaffer have shown, what was crucial for Boyle's success was how he enmeshed experimental and epistemological practices into socio-political ones. Not only did Boyle perfect experiments with vacuum pumps into experimental theatres with large audiences, but he also donated his instruments to prestigious research institutions and taught how the demonstrations can be replicated by others. Finally, this educational influence was still later standardised and kept in quality with Boyle's insistence on detailed reporting, precision in illustration and honest reporting of mistakes and failures. While those principles should not be surprising to many people working in research or academic publishing, keeping them in mind is

important as the problem of public understanding of cybersecurity science grows in complexity.

What I want to emphasise by bringing up Shapin and Schaffer in comparison with stabilised instability is not just the similarity in general principles of accountability and rigour between different experimental sciences. No, Boyle's case matters more for cybersecurity for a few other reasons. Firstly, in my understanding, stabilised instabilities are the social equivalents of demonstrations in experimental theatres. They are often the "news of the day": gossiped among workplaces but limited in exact understanding. They contribute to anxiety or temporary political decisions, but only rarely seeing equivalents of full public understanding and public closure.

As an example, consider the case of the use of Pegasus, an offensive cybersecurity tool that was purchased by various states (including Poland, Israel, Mexico, Indonesia and others) and used to wiretap political opponents and legal protests (Richard & Rigaud, 2024). Pegasus was revealed by the effort of an investigative journalism collective, Forbidden Stories, and security laboratory, Citizen Lab (Marczak et al., 2018). Pegasus operated exactly on the principle described in the definition of stabilised instability: nation-states bought publicly unknown vulnerabilities in digital infrastructures and "fired them" at targeted opponents. Because vulnerabilities were not known (zero-days, as discussed in previous chapter), the victims of the surveillance did not know about it. The companies that provided mobile services and the cell phone manufacturers did not know. After journalists and researchers released their materials, the European Union Parliament ordered an inquiry (Mildebrath, 2022) followed by an inquiry committee in the upper house of the Polish Parliament. The latter finished its proceedings in 2023 (Komisja Nadzwyczajna ds. Inwigilacji, 2023). However, the lower house is still proceeding with its own committee as of 2025. So to sum up: even in the case of a well-documented use of stabilised instabilities against political opponents in such a nominally democratic country as Poland, with a membership in the European Union and NATO (with all their flaws and caveats), it has been seven years since the publication of an otherwise replicated and uncontested security research paper (2018) and three years since a successful inquiry of EU's Parliament (2022), yet the general public is still without closure either from a joint parliamentary report or court trials.

This is exactly why I mentioned the concepts of performative and anti-structure by Victor Turner (Turner, 1995, 2008) earlier. Stabilised instabilities, at least when they become public affairs (as I will discuss later), are public theatre performatives. As such, they are anti-structures, so they become negatives of security theatres as thought by Schneier. Stabilised instabilities as anti-structures translate to not only opening in a disciplinary field as cybersecurity establishes itself as a science, but they may also contribute to changes in social cohesion and boundary between familiarity and anonymity.

What exactly do I mean by that? Stabilised instability, as I defined earlier, is a challenge to the infrastructure. It exists in the context of disruption,

destruction or putting infrastructure and social order in doubt or vulnerability. When such contexts become known to the public, social order related to the infrastructure may also be put into doubt as well as individual meanings, resources and other relations. An example of the social order put into doubt would be the consequences of public disclosure of classified data and dismissal of public officials (as happens in sociological fairy tales but not in reality). Examples of individual meanings, resources or relations put into doubt are the leaks of accounts of adult or dating websites. What is important from an anthropological or sociological perspective is the fact that the public or general knowledge was challenged at what is in anthropology called a liminal stage (Van Gennep, 2019).

In other words, scientific discoveries, especially public reveals from cybersecurity by definition destabilise public order, by making people lose their sense of belonging, or what my friend and a philosopher of technology Andrzej W. Nowak calls "a horror in ontological imagination" (Nowak, 2016). Through challenging established epistemology in various scientific debates and, for cybersecurity, reliance on digital infrastructures, sciences make people feel "neither here, nor there", as epistemological displacement catalyses social and ontological doubts. What van Gennep proposed for the ritual of adulthood, Turner understood as a ritual of cohesion and decohesion of society, hence the theoretical dialectics of structure and anti-structure. When stabilised instability becomes a public affair, as was the case of Pegasus, it also becomes a sociological anti-structure: an opportunity to contest not only an epistemological assumption about security knowledge but also social and political assumptions about democracy, various parliaments, markets, etc.

In this paradoxical way, stabilised instability constitutes a socio-psychological double bind. Scientists, researchers and cybersecurity professionals research stabilised instabilities because these provides them with a sense of meaning, an emotional payoff for satisfying their curiosity or always returning for the experience of "having the root" (being in total control, total power and knowledge of the system). Curiosity-satisfaction, sense of control and dopamine-rush from challenge are, of course, not all the psychological motivations for doing scientific work. Especially after 2020, with the rising standardisation and the rising needs for insurance and certification, more interviewees, especially from student-centred events, mentioned money and prestige as motivators. I discussed it in the previous chapter in relation to Maxigas and Söderberg's concept of recuperation of resistance and hacking culture by institutions (Söderberg & Maxigas, 2022). Regardless of the psychological motivations of individuals within the field of cybersecurity, the double bind on the broader, social scale is to create more uncertainty and social anti-structure.

In my personal interpretation, cybersecurity is not alone as a field in this Faustian bargain between certainty and doubt. This dialectic is a part of the social role of science, since science began to replace religion as a source of justification or meaning for public order. To attempt to discuss any type of knowledge in public, to put it into open, experimental and

repeatable verification is to accept that debate in scientific knowledge will cause turmoil. It is naïve to expect that any kind of science will be free of such responsibility.

This is the final interpretation of stabilised instability. If cybersecurity, at least occasionally, becomes an issue of public scientific controversy, then such controversy would not be resolved only through a debate among experts. Stabilised instabilities reveal issues of power over societies, not only because they epistemologically and materially relate to digital infrastructures but also because they relate to social order, issues of trust, privacy and control. This is the definition of the social role of cybersecurity as a science: if cybersecurity is to become a science that circulates stabilised instabilities, then it should concern itself with public participation, accountability and responsibility. Replication, methodological excellence and digital methods are not enough to make a leap from 1930s science to contemporary science.

Public oversight and ethical accountability are necessary, as Auschwitz's medical experiments, Tuskegee's syphilis study, Wendell Johnson's negative reinforcement experiment and numerous other harms done in the name of science have proven. Why should we expect cybersecurity to be different? If it experiments with larger-scale infrastructures that concern social groups, why should we place different ethical demands on it? Virology and nuclear physics are also closely adjacent to military institutions, but they still have some civilian and professional oversight.

Who should provide oversight over various practices of cybersecurity and its experiments? This is a social, ethical and political question as much as it is an epistemological one. Discussing cybersecurity as a science, one cannot escape it. Not because cybersecurity is ubiquitous, overreaching or special, but because the very same question must be answered for every other field of science.

In the end, interpreting stabilised instability has led to a sociological equivalent of an ouroboros. The more I tried to analyse the peculiarity of stabilised instability as an epistemic object, the more elements common to other relations between other sciences and societies I found. In retrospect, this is not surprising.

Being close to the tradition of C. W. Mills in sociology (Mills, 2000), I know that analysis of individual characteristics often leads to recognition of repetitive, structural or historical patterns. Finding these patterns is a clear sign that it is high time to apply my concepts to some cases.

## Vulgar Display of Power (Elite). Why Does Cybersecurity Science Matter?

How to find a case for global conceptualisation? Many times, I admitted that even such an attempt is incomplete and mosaic by default. The only solution is to look closely at the power elites (Mills & Wolfe, 2000).

Adapting Mills' concept, I understand a power elite in the context of cybersecurity science as a set of social relations interlinking three major power roles: military (including intelligence and state-level law enforcement), political executive and business (Mills & Wolfe, 2000). The roles in those domains are held on a temporary basis, and members often are not aware of being a part of the elite. What is shared is the educational biographies and informal social clubs (here comes the importance of clubhouse mechanisms as discussed in a section on discrimination in the next chapter).

Knowledge has a multitude of meanings within the power elite. Firstly, a shared educational background often catalyses entry but often is not enough. Secondly, the elites use knowledge to obfuscate, gate-keep and lead astray pretenders, for example, with systems of worthless certifications, indecisive review boards and unclearly defined standards of excellence. Such standards waste time and effort of the newcomers, while insiders often are instructed in their families on how to circumnavigate or ignore them. Thirdly, knowledge is often used to justify stalling the need for changes, as any bureaucratic decision can be supported by the need for further research on the topic (academic sociology is often called as compliant in this role). Finally, knowledge, when it becomes standardised and replicated in the form of science, is crucial for expanding and retaining political, business and military power. Thus, knowledge is always useful in three institutional domains of power although the uses are not always epistemic or scientific in nature.

What changed from the times of Mills is the role of academia, both as a nesting point for the elite and as a site of one among many contestations. As I write this book, consulting companies significantly have replaced academic institutions as legitimisers and assurance providers for bureaucracy, especially as public funding for research institutions was reduced and cycles of revolving doors between academia, consultancy, NGO sector and politics approaches the sociological equivalent of Moore's Law.[3] Academia is still important, as PhD candidates and fresh batches of postdocs provide a cheap labour force, cheap teaching and new knowledge from basic research (here I follow economical conceptualisations of Philip Mirowski, see Mirowski, 2011, as they prove to be correct in 2025).

Mills critique of power structure in the US during the Cold War is applicable twofold. First: it was brought up when crucial actors for the military, state and business were forming at the dawn of the Cold War. Digital moguls and venture capitalists from 2025 may tell stories of digital homesteading during the 1990s, but Malcolm Harris has shown that military, politics of eugenics and capital concentrated around Palo Alto long before moguls, digital regents or villains of our time (Harris, 2023). Second: Mills explicitly emphasised that the power elite is not a conscious conspiracy, but an outcome of concentration of power and authority within a limited group. Such a group may be internally incoherent and pose competition for itself for most of the time, but what brings it into agreement is the notion of actual public oversight or control.

This is why Mills' description fits so well to so many cases of high echelons of cybersecurity military-business-state. The United States of America is a useful illustration, as its sheer scale necessitates standardisation on a scale that produces enough paperwork to make its power elite recognizable, but the same concept can be applied for any other sub-selection. Similarly, Mills was read and successfully adapted in Polish sociology for describing power elites among military-party-industry management elites with the correction for oversight from Moscow during the period when Poland was a satellite for the USSR. This is not to say that society or protests do not have an agency: those are completely different questions, and Mills' theory has strongly characterised social systems as open and dynamic.

While issues of change, queer and protest will be discussed in the next chapter, I wish to focus on the relation between cybersecurity and risk. For the period covered by this book, the risk turned out to be financial, due to growth of ransom attacks in the form of ransomware. In response, insurance companies started to sell cyber-insurance, as a financial mechanism of distribution of such risk.

Only after this long introduction do the puzzles find their places. Insurance against ransomware forced at least some sort of standardisation and codification of cybersecurity. Insurance operators need standardisation to compare, adjust and estimate the risks. The connection between cybersecurity science and cybersecurity insurance is completely under-discussed in the academic debate (on the side of social sciences), so the best I can offer, with my limited resources, is an excerpt from an interview with a professional in this niche.

> "My day job is in a company that conducts audits for the insurance companies. I will not discuss any actual details, but I can describe how it is different from my previous work as, let me say, as a red team researcher <laugh>. As financial companies offer insurance products against ransomware, they want documentation and standards. Logic may appear to be completely different from the red team job. Here the process starts with the simplest vectors of attacks. I must check and document them. It is boring as fuck. In a red team, I have done it automatically. Here I must do it step by step. The logic is: the insured party must have the basic stuff in place before we can proceed. Basic server maintenance. Good access settings. Ports must be checked. Because if you do not have the basics covered, what are we even talking about?"

*Interview Fragment 4.1.* As cybersecurity becomes a vital part of financial securitization[4], there is a rising need for bonding between insurance markets and efforts in cybersecurity systematization.

In the cited fragment the role of standards is clear. Documentation and standards serve not as exciting and experimental but as checklists to be

validated and baselines to be kept before proceeding further. This is the reverse side of science that is often overlooked: the science of "what is good enough to be a common practice". The science of "what can be reasonably expected from the majority of overworked practitioners".

Insurance deals with risk. Before malware and other cyberattack risks can be insured, cybersecurity must be at least standardised. For a substantial part of the planet, the American National Institute of Standards (NIST) directly or indirectly influences this role. The reason is simple: if anyone uses products from Microsoft, Apple, Alphabet, Amazon, Intel, Cisco, Meta and many other companies, a significant part of the market for those companies is the US. So, the NIST standards play a substantial role in establishing common standards. In this sense, the NIST is the arm of the political power elite. The tool used by this hand is called the NIST Cybersecurity Safety Framework (NIST CSF), and it was introduced in 2014. Some variants of NIST CSF are among the "boring checklists" that informed my interviewee.

To validate my suspicions, I checked recruitment offers in cybersecurity in my region of Central-Eastern Europe. According to commentaries (Sitarczyk, 2025), about 20% of job offers explicitly require familiarity with NIST CSF standards. It is not really that surprising, as Polish cybersecurity standards are openly referencing NIST standards and their updates (Serwis, 2019). Poland is a NATO member, so interoperability is expected, especially considering NATO support for Ukraine. NIST standards are not unreasonable, at least according to the professionals I interviewed.

The NIST CSF standards are also not necessarily the worst possible thing. Certainly, I would prefer if cybersecurity standards were set in a manner more similar to the International Classification of Diseases Eleventh Edition (ICD-11), through international collaboration and under at least a symbolic public scrutiny by the United Nations and a series of investigatory bodies and public panels (details do not matter as it is completely fictional scenario; a treaty on public, international cyberscience control and disarmament lies beyond even utopian fiction). Since it appears politically impossible, NIST appears as the least bad option.[5]

Benevolent or useful as they may be, the new edition of NIST CSF standards will follow the same path to mirror what is described as the "Brussels effect" in the case of General Data Protection Regulation. Brussels effect descriptions can be found in literature on the EU (Mazur & Włoch, 2023). In brief, it describes a planned expansion of limits of political power beyond the institutional boundaries through a mixture of voluntary standards and technology. Both in NIST and in GDPR, the power being spread is mediated through the extension of digital infrastructures.

The Brussels effect, in the case of GDPR, worked in the shadows and without public scrutiny on key decisions, exactly fulfilling the wishes of power elite, as defined by Mills (Mills & Wolfe, 2000). Standards do not push to be accepted. As time goes by, diplomatic, optional suggestions in soft power easily ossify into an infrastructural, immovable standard. Then the power elite that

has oversight of the standard effectively extends its power. All without firing a shot, only by reversing the opt-in pressure known from network science and well-recognised in the sociology of infrastructure (Lampland & Star, 2009). I have not read such a description applied to cybersecurity standards, especially to NIST CSF, but I know my field well enough to recognise the pattern.

The Brussels effect demonstrates how cybersecurity standards explain the reach of power elites beyond the boundaries of the nation-state. Understanding insurance financialisation allows for better understanding of the role of knowledge in the creation of financial instruments that serve for spreading the risk, shifting the profits to institutions that can provide trust and create new mechanisms for financial profit from science and infrastructure.

How does it map to the concept of stabilised instabilities? Cybersecurity science studies stabilise and change the scales of instabilities. Insurance distributes risk, including the risk from hacktivism, cybercrime and other actions, providing possibilities for shifting the blame to individuals or shell companies if necessary. Stabilised instabilities still may stir public opinion, as private data of individuals is leaked or as they are harassed, but only rarely does it lead to public scrutiny. What Shoshana Zuboff (2019) identified as behavioural surplus is but a singular piece by commercial power elites. Cybersecurity is the keystone; as epistemology of stabilised instabilities allows us to divide and combine digital infrastructures, so it allows us to manage states of exception in formations and flows of capital.

This is why understanding the power elites of cybersecurity science is a necessary condition for understanding the political economy of the contemporary world. From AI to health data, from satellites and Anthropocene to cyborgs and queer theory. This is the episteme of power.

## "Such Sights to Show You". Science and the Standards of Cybersecurity.

Insurance was certainly important for commercial power and NIST standards were also important for it, but the exact role and scale of later generations of NIST CSF for insurance is a question for future research.

In this section, I still remain within the framework of the power elite and stabilised instabilities. My goal is still to understand the process that happens between the formalisation of cybersecurity knowledge and its execution as a form of power into a standard. Unlike NIST CSF discussed in the previous section, this time I am interested in standards for gathering knowledge about vulnerabilities (read: stabilised instabilities), systems of threat scoring and methodologies of estimating cyberattacks.

In practice, those standards in cybersecurity industry are understood as Common Vulnerabilities and Exposures (CVE), Common Vulnerabilities Scoring Systems (CVSS) and MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) Framework. All three are organised into separate but interconnected databases, managed by MITRE. MITRE

is a not-for-profit hybrid institution that oscillates between a think tank, a company, an NGO and a government bureau, which specialises in commissioning state resources into research on signals, cybersecurity, communications and similar defence-adjacent topics. This hedging as not-for-profit but non-government, but responsible for managing federal research funds, makes MITRE a perfect illustration of Mills' warnings.

MITRE is responsible for managing of some research project. This is why it is hard to interpret MITRE as anything else but a perfect lynchpin or an interface for translations between military, commercial and state power.

MITRE seems to avoid open competition with NIST when it can, so initiatives like CVE, CVSS and MITRE ATT&CK were developed in compatibility with NIST CSF and other standards discussed in previous section. The difference is symbolic: NIST is formally and administratively connected with the US government, while MITRE has some deniability. This deniability may be enough for simplest public scrutiny or friendliest of diplomats, but sometimes, even this is enough.

I do not wish to claim that I am discovering and breaking new ground in my field, even if cybersecurity often touches issues of power and secrecy. No, those are publicly known facts.

I am doing exactly what other stubborn sociologists of infrastructure did: I sniff for the standards, and I read them. I will be unable to understand the majority of technical information, but I will grasp enough of the institutional and social context to read more and ask for explanations in interviews.

Harry Collins did so with the gravity wave physics (Collins, 2017), adding some interviews. Collins, in cooperation with Robert Evans, calls this social context "interactional expertise" (Collins & Evans, 2009): what can you learn from a social group through being among it, without having actual scientific expertise. It is exactly the contextual knowledge, the "canteen napkin" knowledge. If a sociologist has hostile intent, exactly the same knowledge is often enough to facilitate cybersecurity breaches in the form of social attacks, when the attacker poses as "an employee who lost their badge" or as "lunch delivery for Alice".

CVE, CVSS and MITRE ATT&CK are great litmus tests for such interactional expertise. They are perfect examples of second-hand knowledge, usable repacking of cybersecurity knowledge in forms understandable by managers, policymakers and other members of the power elite without technical background. Of course, all three categories are equally perfect for selling IT marketing word-salad to newcomers, but this is exactly the moment when science blends into managerial jargon.

Here is an example: CVE[6] is important because it is the first reference point for all vulnerabilities. For example consider CVE-2023–23397 (MITRE, 2023). It is a vulnerability in Microsoft Outlook, a popular email program, used in many companies. It was published in 2023 but updated in 2025. The marking CVE-2023–23397 serves as its identifier. If you enter the CVE database, you may see its entry marked as CWE. If CVE could be understood

as exact symbol for the vulnerability, CWE is the marking for the weakness in the infrastructure that caused it. CVSS is the estimation of the danger of vulnerability. Both are nicely translated to a NIST database: the National Vulnerability Database (NIST, 2023). With this double structure, federal institutions and NIST CSF adopters are using one database and MITRE opens another, for crawling, machine learning, AI agents and, worst of all, Polish sociologists. The CVE database was already used for new types of automated modelling (Machalewski et al., 2024) as well as an open shared-pool resource for counter-intelligence defence campaign (SKW, 2025). Exactly this CVE-2033–23397 was used to gain access to accounts of staff of warehouses that manage transports of supplies to Ukraine and to escalate this access to cameras in warehouses. Cyberintelligence and counter-intelligence communiques in NATO countries openly referred to this vulnerability, to assure that Microsoft Outlook is updated to a new version and that the ports to video cameras are closed etc. (SKW, 2025).

But the CVE serves as more than a shared point of reference. A common set of coordinates makes it easier to make comparisons through time and through genealogy of vulnerabilities. Through careful documentation of mechanisms, the attack described above was compared with earlier attacks on Ukrainian hospitals and health infrastructure. In result, the feedback loop of learning was based not only on systematics, as shown in paper, but on authorship and identification of the adversary (Machalewski et al., 2024).

Similarly, because CVE placed each vulnerability within an ontology, clearbluejar shows how, by analysing the parent category of CVEs, it is possible to generalise and compare CVEs to seek patterns and identify root causes through what they called CVE North Stars approach (clearbluejar, 2023). I do not claim that I understand all details on the cybersecurity science side. I do claim that detailed walk-throughs and descriptions like clearbluejar's are equivalents of advanced papers and detailed replication protocols observed by sociologists of science in laboratories in biology (Latour & Woolgar, 1986), physics (Doing, 2009; Knorr-Cetina, 1999) or planetary sciences (Vertesi, 2015).

I do not cite works by clearbluejar here because they are accessible online, and they take up some space. They are not necessarily accessible to people without some technical background or at least interactional knowledge, but they do what science papers should do. Clearbluejar and many other security researchers used CVEs not just to push further the knowledge on already known vulnerabilities.

No, I invoked the case of North Star CVEs and CVE-2033–23397 to show that CVE systematics allowed for an even more rigorous definition of cybersecurity as a science. Not only a science that describes and forensically examines the history of old vulnerabilities, to discover new mechanisms in old attacks but a science that uses this knowledge to anticipate and create hypotheses about the future.

Those hypotheses are rarely formalised in a style recognised by philosophical epistemology. They rely on instrumental criterion of science, as proposed by philosophers like Nancy Cartwright (Cartwright, 1983) or Ian Hacking (Hacking, 2001). According to Cartwright (1983), scientific laws should be understood as true precisely within the frame of abstracted models. In this sense, scientific laws are instruments for the construction of models. Reality is messy and complex, so the role of science is not only to understand and develop the use of laws as instruments but, equally important, to understand the limitations of models, boundary conditions and critical cases.

What is a theoretical paradox is the fact that cybersecurity by definition is interested in limitations, boundary conditions and critical cases, similarly as immunology is interested in response of the body to abnormal and how science of material failure and fatigue studies exactly what material science wishes to avoid. Knowledge pursuits as those that are symbiotically, or if you prefer your thinking dirtier, dialectically, bound to construct on each other meta-layers, that accrue like a structure of a fractal. Each knowledge relies on the knowledge about its exceptions, failures, and boundaries, exactly in the same manner as identified by Ludwik Fleck as a social mechanism of a thought collective discussed in Chapter 2. To constitute science is to provide working mechanisms of discerning statistical noise from genuinely novel paradoxes.

In this sense, cybersecurity is a meta-science for electronics, computer science, cryptography, automatics and many other adjacent fields, sociology and psychology notwithstanding. It is so because cybersecurity is standardising and researching exact points of failure, or conditions for stability, for situations which other fields may consider practically irrelevant, unsearchable or on the points of failure of modelling parameters.

This is why instrumentalism was found so useful as a philosophical approach for cybersecurity as a science (Spring & Illari, 2019). At the first glance, it defies sane logic, as it proposes that science does not explore reality, but only a simplified version of it. Even worse, instead of the truth (whatever it may be), science is judged by the criterion of manipulating this simplified version of the world. In practice, it allows not only to frame cybersecurity research as research on models, instead of "being just cataloguing and discussing historical cases" (paraphrase of an informal speech). What is no less important, it provides a practical way of removing cybersecurity research from contradictions, ethical doubts and other concerns around performatives of stabilised instabilities in the public.

This is why CVE is important. Not only because it brings a new generation of research, especially in the age of AI, but also it provides a gateway for demarcation, or for separating socio-political contexts from the scientific problem. By framing a vulnerability or a security problem through CVE, managers of the systematics are able to decide what socio-political contexts are included as relevant to research and what are excluded. This is how standards

were understood as political by Leigh Star and her co-authors (Lampland & Star, 2009), not simply because they are important but because they separate what can be left outside the context of the categorised data and, by extension, from the research and infrastructures that build on such data.

The demarcation power of standardisation bodies is, thus, gatekeeping power in a very direct sense. Who can appoint the institution that can validate CVE numbers? Who can inspect CVE ontology and propose changes that would be actually taken as serious? Who decides what will be disclosed to the public about a CVE, and what will be left in the backrooms? In the case of the CVE board, all its members are US citizens, despite the fact that CVE is used globally. This is a peculiar variant of the Brussels effect, as the standardising body is not operating within the recognised boundaries of the nation-state. Since MITRE is based in Virginia, "the Virginia effect" seems like a fitting name.

As a variant of its Brussels counterpart, the Virginia effect is an extension of the state's political power through a formal voluntary standard proposal in the domain of digital infrastructures. In the case of CVE, it moved from nebulous concept about 25 years ago to an accessible and vast ontology that allows automated cybersecurity research or defence. Similarly, the Virginia effect starts as a social convention or a conversation about a systematic in the form of some reports or briefings. As time passes, it ossifies into material infrastructure itself, achieving the benefits of a network effect. Even if other parties are unsatisfied with the details of the standardisation, systematics like CVE become too useful or too common to ignore. Hence, what was an epistemic proposal turns out to be a direct political power of the state or company.

Luckily, it is still possible to investigate one of the documents that most likely lead to CVE as it is understood today. Around 2010, MITRE was tasked by the U.S. Department of Defense to prepare a report and series of briefings on cybersecurity as a science. MITRE gave this task to JASON, a group of scientists created during the Cold War to advise in matters of national defence and similar. JASON's report has been made public with the signature JSR-10–102 (JASON, 2010). Working on this book, I did not have enough time to reconstruct the details of relation between JSR-10–102 and changes of the CVE standards, but as both originate from the same department of the same institution and as both share some involved parties, like NIST representatives for cybersecurity, some theoretical feedback likely took place.

If CVE is the standardisation offered for cybersecurity specialists to use, then JSR-10–102 can be read as an exercise in the application of a theory of science. If CVE is the Virginia effect and everyday practice of cybersecurity emergency teams, then JSR-10–102 is the debate on the epistemology or on the ideal. JSR-10–102 was not written by theorists, though, but by academic researchers with practice in the industry and delegates from military research institutes with experience in companies. Similarly, CVE has a sophisticated ontology of information, so it would be a grave mistake to disregard it as "mere practical application".

Neither JSR-10–102 nor CVE or CVSS were the first attempts to systematise cybersecurity. That is not my claim. This book is not an archaeology of knowledge nor a historical study but a study of a certain period. For the sake of clarity, I also will not discuss in detail all the briefings that constituted JSR-10–102, even if they differed in perspective. A significant part of such comparative analysis has been done earlier within philosophy (Spring et al., 2017) or within the field itself (Herley & Van Oorschot, 2017).

A debate on the JASON's report was continued in philosophy of science and philosophy of technology, notably through the papers by Spring and co-authors; by reducing JASON's statement to a "problem of common language", they missed important pieces in their model of mosaic unity of cybersecurity as a science. Spring and co-authors correctly translated the philosophical concept of mosaic unity into a sociological model of a multitude of trading zones (Galison, 2010). Returning even further to empirical research on this concept, there is a work of Peter Galison on physicists, engineers and electronic researchers that interact around experiments, instruments and theories (Galison, 1997). This is not an issue of academic pedanticism, trust me. The division between experiments, instruments and theories was crucial for Galison's explanation, as each of those objects allowed for at least a temporary stabilisation of the trading zone. Stabilisation not in the sense of stabilised instability, but in a biographical, social and epistemological sense: continuity of manuals, continuity of careers, continuity of funding. When one theory was disproven or when a precise instrument failed, the lab relied on the fact that it still shared an understanding of the experiment details well enough to share it with the close mosaic but unique enough to be still indispensable. The instruments, theories and experiments were boundary objects (Star & Griesemer, 1989) that facilitated the translations between trading zones. The socio-epistemic mosaic had boundary objects as miniscule grains, which both facilitated exchanges between labs and subgroups and allowed for stabilisation during moments of epistemic discontinuity.

To philosophers, this may appear as minutiae or nauseating bookkeeping from social sciences. It is so easy to abbreviate common concepts and common standards and other things enumerated by JASON to just "common language". But this is why tracing sociological work of Susan Leigh Star and their co-authors matters and is so practical (Star & Griesemer, 1989). Boundary objects are common in mosaic unity not because everybody ascribes them a similar and unchangeable meaning. No, boundary objects, such as theories, experiments and instruments are common because they are in-between the social interactions of groups. They allow for maintaining stability of a lab, or the stability of a career or the stability of a project even if a mosaic becomes unbearable as a vocation elsewhere. Peter Galison openly referenced it and focused attention on those issues (Galison, 1997).

In my understanding CVE, CVSS and MITRE frameworks are exactly those, the "boundary objects", stabilised instabilities. They are not common languages, if that would necessitate universal understanding, but they

are common enough for the scale of localised understandings within the mosaic. What is necessary is only local stabilisation, just for the lab, for the project, until the child grows up. This stabilisation itself was enough to advance with experiments and the falsification of hypotheses, which fits even logicist-empiricist criteria.

JASON thought around complex epistemic models. They compared cybersecurity not only to physics, mathematics or cryptology but also recognised that attack-defence feedback loop models well into epidemiology, immunology and agriculture sciences. The basic conclusion from those comparisons was the fact that security degrades over time. No less importantly, JASON already speculated about automatic proofing and using virtual machines as sandboxes for running suspicious software in an isolated environment. This can easily be compared to recognising the importance of bench glove boxes or isolation chambers integrated into a bench: what may appear as a mere logistical switch results in a revolution in practice.

Privately I may be an atheist, Marxist, critical sociologist, but I come from Poland. This is why I would not be myself if I had not found not one, but two devils in JSR-10–102, as it is commonly known,

As I read JASON's report, I recognised the name of Peter Galison. I discussed how his work was relevant for cybersecurity as a science, and I read his work as a PhD candidate. I was somewhat surprised that Galison briefed JASON and MITRE not on any sociological or historical theories I knew but on what was, at least in fragments, a political theology of cybernetics. The formal title of the briefing was "Augustean and Manichean Science", and it is a reference to Galison's research on Norbert Wiener (Galison, 1994). The metaphor from theology was called to illustrate what is an unresolvable, but cognitively fruitful, epistemological dichotomy. So, I am interested in it, not to answer whether anyone present in the JASON briefing believes in the devil, but to investigate what political and social associations it brings to the debate in cybersecurity.

Details of this theological duality will be explained in a moment, but, before that, I wish to explain why I believe they may be significant in 2025. In other papers, cybersecurity also recognised the epistemological presence of an adversary. How this adversary is imagined, as an epistemological figure and from what traditions of sources the thinking about the adversary is taken, matters for the field.

Norbert Wiener was a pioneer of cybernetics research. Galison discussed Wiener's work because of his particular insight on adversarial modelling (Galison, 1994). When Wiener was developing a system for controlling gun turrets for American bombers, he modelled the response of the targets, a system of fighters and their pilots effectively as singular adversaries. Trying to understand this element of the feedback loop, Wiener called back to Christian theology for the distinction between devils as figurations of such an opponent.

The devil in the religion of Manicheanism, later considered a heresy by Christianity, is a rational adversary. A Manichean devil tries to outwit, trick and conceal its intents. In contrast, the devil according to Saint Augustine is disorder, entropy and chaos. While the Manichean devil could and would change its tactics, the Augustinian devil was unable to change in a manner other than random.

This illustrates the fundamental duality of the adversary in cybersecurity as a science. Is the adversary just the disorder, a random failure, or is the adversary cunning and always concealed?

As it was the case in the times of Norbert Wiener and Charles W. Mills and is today, theological considerations find their appeal among the power elite. It may not be intended as a goal of JASON's briefing in 2010, but, in 2025, Wiener's thoughts may find more than a few aficionados among the Silicon Valley elites.

Wendy Chen, in her ethnography of elite software workplaces in the Valley, found that para-religious fascination with mindfulness and similar practices goes beyond the need of relaxation or occasional spirituality (Chen, 2022). As observed by Chen, software companies recognised that employees may be attached to a "spiritual" meaning of work, so they started to bind religion with coding. The purpose is the same as in every binding of religion with the workplace: to make people work more willingly for less or to make them accept conditions that they may not accept otherwise. When it comes to brainwashing in the workplace for the sake of some research, religion is almost as good as academia (hey, the social origins of both are the same!).

It is important to note that such ideologies and social practices were observed and described by Chen even before the AI investment boom swept the labour landscape. The AI boom, supported by the cryptocurrency period gave rise to the TESCREAL[7] as described by Émile P. Torres and Timnit Gebru (Gebru & Torres, 2024). TESCREAL could be sociologically summarised as vortex of ideologies that lure through the promise of meaning by reference to transhumanism, eternal life, crisis of humanity, machine-gods, eugenics and the future of humans (read: the white-rich-able bodied-IT-Valley-based).

The TESCREAL cosmogony is unclear and functions as a honeypot in its own right. It lures through novelty or absurdity, only to gradually shift its meaning for some readers, in a way similar to climate denialism or flat-earth theories. This is why I abstain from discussing it in detail.

It is a mistake to consider either Silicon Valley or the American power elites as secularly technocratic or completely atheist. Religious imagery plays an important symbolic role not necessarily as direct religious symbols but as other types of boundary objects; this time necessary for at least a temporary ceasefire and negotiation of support or funding. My professional specialisation is too far away from American Evangelicalism or Christianity in general,

or its influence on Conservatism, to discuss it in more details, but it does not mean I will be blind to what is obvious.

## Summary

In this chapter, I proposed how to theorise computer security vulnerabilities as quasi-theoretical objects. They are theoretical, as they always exist as some sort of abstraction or proposal. They are quasi-theoretical because they depend on computer infrastructures to be discovered or to act. They are also performatives in the sense of Turner's theory and in a long legacy of history of experiments.

Without an audience to witness and verify how new instabilities differ from the existing ones and without validation from cybersecurity profession or science, instabilities exist only as hypotheses or notifications, but not as facts. This is why an untested, unknown zero-day lies on the boundary of this concept, similarly to an untested scientific instrument.

As a stabilised instability becomes performed, it also becomes a social fact. Infrastructures are tested or breached. The public may be informed or agitated, but only rarely will the public outcry result in counteraction. This is how cybersecurity is political as a science, through stabilised instabilities rearranging the boundaries of social trust, privacy and visibility in the public sphere, not just through abetting the targeting of individuals for digital services or for missiles fired from drones. Shoshana Zuboff's concept of behavioural surplus (Zuboff, 2019) can be read as an individual dimension of the social implications of cybersecurity as a science. Important and painful for the individuals affected directly but insufficient for understanding the implications for the non-affected.

Through an understanding of stabilised instability, this chapter discussed cybersecurity systematics, deployed in an official nation-state capacity as NIST CSF and proxy tools of what I called the Virginia effect: CVE, CVSS and MITRE frameworks. Illustrating standards with examples from literature and fragments of interviews, I have shown how cybersecurity creates knowledge. By discussing examples of CVE research, I have also shown points of agreement and critique with existing philosophical proposals on cybersecurity as a science. I agree with the adoption of instrumentalism and mosaic-unity as first-degree philosophical approximations, but I remain critical of international, public unaccountability in terms of ethics and on the issues of trading zones and boundary objects.

Contrary to the existing philosophical literature by Spring and co-authors (Spring et al., 2017), this chapter argues for studying classification systems such as CVE or MITRE frameworks as boundary objects necessary for the effective functioning and examination of trading zones or the mosaic. It is my understanding that CVE act as a common language and common material, as envisioned by JASON, and put into doubt by Spring and co-authors.

However, the paper by Spring and others on JASON's report remain a pivotal contribution in the philosophy and sociology of the field. Further debate on later philosophical-cybersecurity papers (Spring, 2023; Spring & Illari, 2019, 2025) remains open.

Finally, to discuss how cybersecurity knowledge is developed in separation from democratic control, I discussed the results of my epistemological reconstruction through the framework of Charles W. Mills' "power elite". Showing that cybersecurity is concerned exactly with the opacity, transparency and accountability of power-knowledge institutions, I have revealed how cybersecurity as a science is developed as an instrument for the power elite of the United States of America.

The US does not have a monopoly on the standardisation of cybersecurity knowledge, so the European Union launched its own equivalent of CVE, European Union's Vulnerability Database (ENISA, 2025). Similar databases likely exist or will start to exist in spheres of epistemological influence of countries such as China and others. There are also databases that are nominally maintained by non-partisan, international bodies, but CVE remains the largest and most influential.

This is why understanding the political theology of Augustinian and Manichean devils, as discussed using MITRE briefings and Peter Gallison's research, remains an important element of understanding cybersecurity relevance to the TESCREAL bundle of ideologies as well as to sociological research on religion among the elites of Silicon Valley and the computer industry.

Reconstruction, examples and theorisations given in this chapter definitely do not provide the full picture of the field on a global scale, nor even in the context of the US sphere of influence. Being critical to the power of CVE and other under-examined standardising bodies, I cannot escape one final irony. Through this chapter, ultimately, I share the same hope: while the socio-epistemological model given in this chapter may be false, I hope that it will become useful.

## Notes

1 To be precise, I am simplifying two venues of Turner's thinking into one: one about anti-structure and the role of play within social action (Turner, 2008) and one about performance and its role (Turner, 1995). Fortunately, both lines of thinking are not mutually exclusive but complementary. One should remember that the unspoken coordination and negotiation of acceptable rule-breaking in performative social actions is a complex question in social and cognitive sciences (Chałupnik, 2023; Muntanyola-Saura, 2022).
2 Theoretical simplification and abstraction used for clearer explanation of a concept that in real life does happen in that clear form. It may be understood as sociological, Weberian ancestor of a persona used in cybersecurity, digital marketing and IT in general.

3 It is a generalisation, but at least for G20, I could not find a country without a major corruption scandal with public IT procurement for the period 2014–2025.
4 I understand securitization of cybersecurity as the development of securities and insurance markets designed to underwrite cybersecurity threats. Securitization of cybersecurity was recognized in actuarial sciences, but has not been explored in social sciences covered by this book. By turning attention to this fragment, i wish to contribute to the existing gap in knowledge.
5 I know that ISO 27001 exists as well as several others. The key issue lies not only in the genesis of standards but in the political will of key state actors and their power elites. Network effects, remember?
6 Systematics like CVE, CVSS and others deserve a dedicated project in science studies. This short section should be read as an introduction to the topic for my colleagues who study cybersecurity in social sciences.
7 TESCREAL is an acronym from ideologies: transhumanism, extropiansm, singulitarianism, cosmism, rationalism, effective altruism, and longtermism. If even the acronym is composed from several nebulous, morally laden and utopian concepts, then it is easy to forecast charity galas, tax-exemptions, and beautifully abstract mathematical modeling. It has led to bad consequences, from genocide fantasies brought to rich donors up to cases of workplace self-harm and murder. As one can imagine, apocalyptic para-religions, masses-be damned, "let us consider eugenics" cults rarely turn out to be communities of care in the long run.

# 5 "Subversions."

## Discrimination. Queer Cybersecurity. Feminist Cyberlaw. Reflections.

Throughout the book, I discussed groups in cybersecurity on different scales of geography, formality and institutionalisation. Geography impacts cybersecurity not only through limits of boundaries of nation-states but also on a regional level. For example, different waves of popularity or activity of hackerspaces are related not only to the global outsourcing of labour but also to the local gentrification processes. Free laboratories, hackerspaces or other informal meeting points for cybersecurity groups were often used as stopgaps before city space could become turned into more profitable property. Formalisation and institutionalisation processes are interlinked, but each does not have to follow the same direction as the other. For example, when a local university hosts informal talks for DevOps (see Chapter 1), these informal meetings may act as probes for a living lab or another more formalised science participation. Conversely, it is not unusual for academic or business institutions to deliberately develop less formalised zones as a form of local networking, PR for interested cadres or as recruiting pools for contractors. One example may be Google Campus. Another example may be monthly events such as lab open days, intended exactly as a trading zone between academia and practitioners.

In this chapter, I wish both to correct and to show the limits of generalisations given in previous chapters. Formality, institutionalisation and geography will still be important, but my focus will not be on the trading zones or on the process of farming on informality for the benefit of more structured actors.

In this chapter, I am interested in practices that challenge the interests of at least some members of the power elite. What follows, I am also interested in practices that do not fit neatly in the reconstruction given in the previous chapter. I wish to examine at least a small subset of practices that challenge the power elites from within the field as from the outside. As in all cases in this book, that list is incomplete and should not be read as definitive or even representative.

Understanding alternative or transformational practices is important sociologically. No field of knowledge is static, and no field of knowledge goes without an attempt to challenge, queer or redirect its social composition.

DOI: 10.4324/9781003396871-6

Understanding those social counter-currents is thus necessary for the goal of the book. As any abstraction of the infrastructure, social structure should not be considered as meaningfully understood without what I called stabilised instabilities. In this spirit, this chapter ends my book with an attempt to apply my theoretical concepts as tools for reflecting on my own ethnography. If not for better reasons, then to open up my thinking to alternatives, cracks and failures, similarly to how digital infrastructure has to undergo a thorough exposure for testing.

Throughout the research, interviewees used different pronouns, different genders, ethnicities and places in workplace. Marginal and non-hegemonic perspectives matter, as it is epistemologically important to show that the power elite does not have total control over cybersecurity as a field of science.

By necessity, each section will be closer to a vignette than to longer theorising. Instead of theorising about exclusion, queer or ethnic discrimination in the workplace, I prefer to say how this ethnography may contribute to each of those perspectives.

The first section discusses an ethnography of cybersecurity labs in the context of various forms of exclusion from science, technology, engineering and mathematics (STEM). Exclusion may come from gender but also from ethnicity, wealth or psychological factors. The second section discusses a case of queer hacktivism to highlight its importance for developing concepts for a public understanding of cybersecurity science. The third section gives a small vignette on the connection between cybersecurity science and individual emotions of researchers. The last section discusses the project of feminist cyberlaw, focusing primarily on similarities in ethical commitments between feminist cyberlaw and examples discussed in earlier sections.

## Clubhouse Strikes Back? Social Mechanisms of Exclusion Between Formal and Non-Formal Education in Cybersecurity

When any field of science becomes close to power or money, different forms of social exclusion follow. Often discussed gender-based exclusion is not the only kind, nor does it provide a universal blueprint for investigating exclusion of ethnic minorities or exclusion based on class.

Since this section aspires to intersectionality (Collins i in., 2021), I share the following perspective from gender studies of science. Different regional contexts shape understanding between feminism and science (Eren, 2022), because feminist thought is what people relate with, use and refer to in their actions and not a systematised, universal corpus of knowledge.

Within this intersectional perspective, what seems to repeat between different kinds of experiences of discrimination as reported by interviewees can be understood as the “clubhouse model”. Within a clubhouse exclusion mechanism, discrimination comes from two mutually reinforcing sources

that together structure self-efficacy, motivation and other individual factors (Msambwa i in., 2025) impacting both formal and informal education.

The first source is difference in access to experimentation. This is understood not simply as access to the laboratories or equipment but, more importantly, as social acceptance for failure, misuse and unexpected use of computers, instruments, etc. This is important because failure and punishment for it contributes to the sense of self-efficacy, which is recognised (Wong, 2016; Wong i in., 2024) as a psychological metric intersecting the impact of colleagues (Toh & Watt, 2022), perception of self-belonging (Veldman i in., 2021) or career aspirations in the high school period (Hamer i in., 2023).

The second source comes from the function of role models, understood both as cultural references and as a structure of social contacts with people more experienced in the field (Hamer i in., 2023). For example, even in a case as favourable as an individualised mentoring program for girls in STEM, survival analysis has shown that mentees with access to a program-wide network of support and information were less likely to drop out of the mentorship relation than those with a single support. In other words, it is not only about role models, or even mentors, but also about the ability to validate the individual perception of hardships with others and to learn from the experiences of peers. Mentors matter, but they matter the most when mentees can talk about their personal issues, including issues with their mentors, with other mentees.

Both sources occurred repeatedly throughout the talks and interviews with women security researchers as well as throughout interviews with researchers or students of computer security that come from ethnic minorities or economically disadvantaged homes.

> "I dropped out from elite maths studies because everyday sexism was just corrosive. I was tired because I felt that my failures are also accounted as a sign of inability of the whole 'women's team'. I finished a different degree. Now I work in healthcare IT research, so, more often than not, I have to figure out security or privacy issues, as healthcare IT often has some peculiarities, but because I roll mostly with biomed people, the acrid pressure went off. My mistakes are mine and do not go on the gender-IT scoring board."

*Fragment 5.1* Experience of gender discrimination as reported by a woman working in cybersecurity healthcare IT research. As reported this case, liminal space between two fields offers a respite from discrimination that would have been more present in either.

Consider Fragment 5.1, what the interviewee called "the acrid pressure" is exactly what erodes a sense of self-efficacy, on the one side, and reduces joy and satisfaction from experimentation, on the other. What is also important,

reading from this interview, is that exclusion mechanisms do not have to be necessarily associated with a singular traumatic event. Everyday corrosion of self-efficacy is as destructive as singular events.

While the studies I cited come from general research on STEM discrimination from formal education, I consider the clubhouse model as especially relevant to cybersecurity. Simply speaking, discrimination by "do-it-yourself" or "do-it-with-others" matter especially for this field because, at some point in becoming a cybersecurity professional, one has to solve some security problems on their own, either in code, in law, in documentation or in interpersonal communication within the company.

The name comes from the ethnography and historical study of woman programmers and hackers in a prestigious educational institution done by Allan Fisher and Jane Margolis (Margolis & Fisher, 2003). Margolis and Fisher worked with women computer science degree students from 1995 to 2005, so not all of their findings can be applied in 2025. This is why I interpreted interviews not only through the work of Margolis and Fisher but also through additional reading on contemporary psychology and sociology of STEM exclusion, at least in major reviews.

While the works of my colleagues who studied different dimensions of hacking than gender (Fox i in., 2015; Hunsinger & Schrock, 2016; Lindtner, 2015; Mauro, 2022) suggest that the clubhouse mechanism may also apply to cases of economic, ethnic or transgender issues, I wish to leave my modification of the clubhouse mechanism for further verifications.

I also wish to emphasise that feminist, LGBTQ and other inclusive-minded hacking and/or cybersecurity self-educating groups made a lot of contributions in inclusivity and that in many local, regional and national contexts, institutional or individual discrimination, violence or other forms of exclusion may have different forms and provoke different community responses.

I proposed a simplified model, not to provide an exhaustive account of the experience of the interviewees, but to suggest a tool that can be relatively easily translated into standardised large-scale psychological or sociological measurements or institutional policies by the interested parties. This choice was made in agreement with interviewees who shared their experience on discrimination but preferred anonymity.

## Queering Cybersecurity. Feminist and Queer Vulnerability Research.

As feminist, diversity and queer perspectives gained popularity in mainstream IT, the push for exploration of queer perspectives followed. Understandably, computers have been understood as the space for the second self for young people (Turkle, 2005), a space-time-activity where they could experiment with their identities in interactions. What changed, both in self-reflections of

the feminist activists such as Ada Collective, Gerwani Collective (Wuschitz & Reza, 2021) or Maria Lab and in scholarship[1] (Fox i in., 2015; Burek i in., 2018; Dunbar-Hester, 2019; Dian, 2024), was perhaps the growing awareness that those digital spaces of second selves are not peaceful nor do they universally follow the same social trajectories, as some readers may wonder. Just as clubhouses described in the previous sections, formal and informal laboratories were recognised as seats of power, deeply embedded in the local politics of gender, sexuality, class, ethnicity and other dimensions of political power.

In this short section, I wish to discuss one selected case of cybersecurity research that will also serve as an interesting illustration of the uses and paradoxes of the queer perspective.

Maia arson crimew is a Swiss cybersecurity researcher, who uses *it* and *she* pronouns. Its second name evokes a combination of the words "crime" and "mew". She uses a cat-persona as her identity in interviews, especially when discussing political and individual meanings associated with public disclosure of data. In this sense, recognisable performativity of gender from Judith Butler (Butler, 2015), transposed and subjectified as queer identity into irony of public hacktivism advocacy, blends with performative aspects of epistemic gesture of stabilised instability. Performative of a queer fursona, the cat-person image of maia, acts both as a honeypot and as a trap into an infinite regress of interpretations. It lures attention into issues of public interest like images from video monitoring in Tesla factories, the non-existent privacy of workers in nuclear power plants or monitoring feeds from jails in Alabama.

There is a popular joke or a quasi-open secret that illustrated this struggle for the spaces for the second self as well as the struggle for the trust and ethics of cybersecurity knowledge. As many examples of security or hacking humour, it should not be taken either completely seriously or completely ironic. Instead, it is given as an open, interpretative challenge.

Through the fieldwork, I witnessed many times when a newcomer asked naively: "Why there are so many trans and queer people on this cybersecurity conference?" The answer infallibly followed: "Well, if you grow up with a double identity, secrets and codes appear as a natural profession, don't they? Don't mind the queers. Mind the normies in the room. What are they hiding?"

By and large, I experience discrimination only rarely. Sometimes my accent gets too thick, or my skin gets too dark, and I get sometimes what Eastern Europeans know as "white, not quite" treatment (Kalmar, 2022). Because of my limited biographical standpoint, I had

to rely on interviews to understand queer and minority perspectives that inspired individual researchers in their research. Comparing limited knowledge from interviews with the literature, I believe that subaltern or non-hegemonic perspectives are especially useful as epistemic standpoints, exactly because they cover what was neglected, unmaintained and treated as socially invisible (Rosinska & Pellerito, 2023; Dian, 2024; Basu & Biddolph, 2025).

At least some interviewees of mine from the disenfranchised subgroups reported finding a strange sense of reconciliation in cybersecurity. If digital infrastructures are often so messy, biased and fallible when investigated from the inside, then perhaps their researchers should be less self-judgmental about themselves also?

*Fragment 5.2* Queer perspectives in cybersecurity. Trans, queer or other marginal perspectives often find a home in cybersecurity because, for this field, identity is the weapon and the question.

It would be a mistake to forgo maia's research as relatively simple in technical terms. Maia openly admits that it uses very basic tools, like scanning open ports with software like Shodan or going through leaked accounts that float in the dark web. This relative simplicity has a provocative, exhibitive and invitational value. By maia's practices cybersecurity becomes banal, obnoxious, casual, un-serious. This is collectivisation of knowledge by queering it, to make the knowledge everyday, funny, absurd and accessible. It is the opposition of MITRE and political theology of devils. Yet, maia's hacktivism and research surpasses and queers also the Donna Haraway's cyborg manifesto (Haraway, 2006) or defies the simple definition of a public interest hack by Allison Powell (Powell, 2016).

To regard maia as Haraway's cyborg would be to miss the post-Snowden era and to erase maia's criminal persecution and her deliberate political framing as an anarchist. To frame maia's research into public interest would be to take its anarchism (crimew arson, 2024) as an act of citizenship, which appears to me as unethical.

Maia's hacktivism was prosecuted by the United States legal system. She was sentenced, and an international extradition letter was issued in 2021. Maia openly talked about its fear of imprisonment, which shows that openness about vulnerability may be a sharing strategy among queer, feminist and other cybersecurity researchers, who engage from the perspective of disadvantage. At the same time, emotional honesty and vulnerability are hard to misuse by the judicial system of the power elite, as even ex-FBI profilers get trapped in the honeypot / infinite regress debate I mentioned before (Kappa, 2025). Instead of taking maia's identity as it is and moving to the effects,

influence, political resonance or any other more interesting subject, profilers get lost in layers and layers of irony, camp, pastiche and references to references.

While I do not share their interest in criminalising maia, I can at least reconstruct the perspective of law enforcement as well as of some cybersecurity researchers who refuse to differentiate between hacktivism and a cybercrime of attack on digital infrastructures. It is hard to attribute an action in this field, and even a public declaration is not a proof of the action. Within this framework, queer and anarchist politics are easily discounted as false-flags for the actions of other nation-states or rival factions of power elites.

For example, consider the public panic about the danger posed by China to the technological supremacy of the US. If rephrased in a language of cultural theory, gender and colonial aesthetics that are often associated with the symbolism of a cyborg through debates in the Global North, they were used as a form of gender weaponisation by the attacks attributed to the China Girl Security Team, a large fan-based crowd led by hacker-idols like Xiao Tian. The cyborg-gender performative aesthetics of Xiao Tian spread through social media like a wildfire, drawing attention just like later maia arson crimew did. The attention of the gender-cyborg brought interest not only in the actual attacks, for which Xiao Tian took responsibility, but also inspired her followers to study cybersecurity.

What Long T Bui theorised in terms of gender studies as a reconfiguration of the Chinese woman in the age of digital penetration (Bui, 2015), equally functioned as a recuperation of such performatives by the Chinese state and a play with gender with another power elite, this time seemingly in opposition to the interests of the US.

I do not believe that maia arson crimew did what it did as a sock-puppet or as a smoke screen for an operation of another nation-state. That is irrelevant to my theorisation. What is important is to understand that queer and gender performatives of cybersecurity are also recognised and under recuperation by at least some state actors in scales and contexts that previously escaped.

This leads to a new paraphrase of an older thought by Katherine N. Hayles (Hayles, 2006), this time in the context of my ethnography. Performativity of gender and performativity of cybersecurity blend together, making the figure of a cyborg even more unfinished and elusive than ever.

When cybersecurity becomes science, broken into standardised databases and automated detection systems, queer performatives of cyborgs turn to weapons, counteractions, or obfuscation as well as practices of care.

## Feminist Cyberlaw and Feminist Cybersecurities. In Search of Alternatives.

My project focused on a scientific aspect of cybersecurity as practices closer to mathematics or computer sciences. It would be a mistake not to mention

at least two other aspects. The first one is the concept of feminist cyberlaw. The second, the conceptualisations of feminist cybersecurity in international relations.

The concept of feminist cyberlaw was developed by the group around Amanda Levendowski (Levendowski, 2022). Feminism in this context is understood as emphasising the importance of consent, safety and accessibility.

Levendowski focused on the issues of law particular to the US, such as the Computer Fraud and Abuse Act (CFAA). Levendowski discussed an attempt to make a precedent through an interpretation of the CFAA to make any misuse of Terms of Service of computer software or hardware a criminalised offence. This precedent was brought before the US Supreme Court. What was crucial, Levendowski observed, was the fact that the US Supreme Court declined to consider "exceeding authorised access" a federal crime.

This left a wider gap for labour activism, anti-discrimination research and cybersecurity research but made it harder to persecute unauthorised disclosure of naked pictures or to act against stalking, which often combines real-world tracking and violent fiction. Despite political changes, Levendowski's project gathered interest from other scholars and practitioners, which recently led to an edited volume (Jones & Levendowski, 2024), which expanded on feminist cyberlaw theory on fundamental issues like race, abortion and disabilities.

What is important is to notice that the principles of consent, care and accessibility were successfully used in a legal discussion made in close connection with a relevant technical context. This shows that feminist ethics inspires not only social theory or other abstract macrosociological issues but also everyday, practical issues like the application of law for victims of stalking, women surveilled in their smart homes (Slupska, 2019) or people experiencing discrimination.

Very similar issues were of interest to researchers in the domain of international relations. They proposed feminist cybersecurity as a perspective for investigating radicalisation of international terrorist groups around fantasies on violence against women (Armstrong, 2021; Bengtsson Meuller, 2023) or on the online stalking and community enforcement of gender norms, surveyed through cybersecurity devices (Mhajne & Henshaw, 2024; Mhajne & Whetstone, 2024, 2025). Feminist scholars of cybersecurity in international relations emphasise the necessity to understand cybersecurity outside the institutional boundaries of nation-states, which only emphasises the need for multi-sited, intersectional and multi-situated research.

## Instead of an Afterword

The first ethnographic notebook used for this book comes from October 2014. It contains notes from observations and a few spontaneous talks from one hackerspace. The last conversation comes from July 2025. It was about AI slop, or the massive submissions on vulnerabilities done by large language

models (LLMs). It seems like an epoch between a post-Snowden moment, when surveillance became briefly the topic of the day, and a current moment, when cybersecurity is considered as much as a tool for economic enclosure as for discovery.

From this period, I wish to subjectively emphasise three issues. First, the discourse about the Internet and cybersecurity in particular is caught in a strange Groundhog Day. On one side, almost nobody, except perhaps for lobbyists and their academics, believes in tales about an apolitical Internet, as issues like the Brussels effect or digital feudalism appear in opinion pieces. On the other side, there is a strange comeback of 1990s discourse, as if AI found some unused reserves of Web 1.0 and 2.0 propaganda. Cyberpunk Gnosticism also comes back. Perhaps this is the moment to admit that even in digital sociology, history does not repeat itself, but it often rhymes.

I believe that this somewhat nauseating repetition of marketing discourse actually covers the fact that cybersecurity has advanced into systematisation, standardisation and professionalisation. Systematics like CVS allowed establishing shared understanding and has automated at least some of the security tools. Standards, like protocols used by cybersecurity insurance investigators I had interviewed, contribute to what is currently known as "privacy professionals" (Birnhack & Mundlak, 2025). In effect, recuperation, or the business recapture and commodification of the hacking culture, becomes normalised. It does not matter that all recuperated practices become internalised into institutions, as I have shown in the case of CTFs, as common grounds shared between siloed institutions are still incredibly useful. Additionally, what is done in the spirit of a shared passion for cybersecurity may escape remuneration for labour, exactly like some cyberprophets of 1990s used to forget.

A second recognition comes as a consequence. The process of commodification of culture into unpaid labour has been identified as the "Californian Ideology" by Richard Barbrook and Andy Cameron (Barbrook & Cameron, 1996). What I wish to emphasise is how the current wave of Californian Ideology, while influencing epistemologies of cybersecurity as a science, actually turned into various forms of theology. Unlike previous conceptualisation, this time it is not about "new age" or "1968", whatever one wishes to associate with those, or even some gnostic undercurrents from popular readings of cyberpunk, as understood in Cyberpunk 2030 or in the Cyborg Manifesto (Haraway, 2006), but from political theology of the right-wing Christianity and Judaism that has been so useful for the power elite.

In the fourth chapter, I discussed Peter Gallison's research on the influence of Christian theology on cybernetics as science in the presence of an adversary (Galison, 1994). JASON's report looked back at this research, as it conceptualised the same problem for 2010s cybersecurity science: how to construct an epistemological model of the enemy? Palestinian feminist scholars of surveillance independently recognised that theology, this time Jewish, underpins surveillance and cybersecurity operations of Israel in Gaza (Rouhana &

Šalhūb-Kīfūrkiyān, 2021). Nādira Šalhūb-Kīfūrkiyān calls this "security theology" (Šalhūb-Kīfūrkiyān, 2015), when the imagined space around cybersecurity becomes untouchable and inaccessible and can be only discussed by the initiated within a hermetic order. Outsiders have only religious metaphors, but through every metaphor, the power of the initiates only grows, as do prices for their products. Paradoxically, this goes against many ideals of hacking as well as against the ideals of science. Science is not the arcane, hermeneutics; it is not for the gifted or initiated, but it should, at least in principle, be understood universally. I guess that I have only one conclusion: the struggle about ethics in cybersecurity is the same as the struggle about ethics in science (Wolfe, 2020). This set of political theology is colonial, as it sets cybersecurity as a guardian of holy secrets of the state, as an uncrossable divide between conquerors and subjects of the conquest, between the "sec people" and "lay people". When I write holy, I do not mean that I believe that there is anything supernatural in knowledge, nor that I even think that people using this rhetoric believe so. I write "holy" in a Durkheimian sense (Durkheim, 2008), understanding cybersecurity as "holy" means as separated from everyday life as social taboo, imposing a set of rigours on the society, the justifications of which lie not in evidence but in performative rituals.

At the same time, cybersecurity science, in the very non-religious and completely scientific, non-metaphoric sense, acts as the locksmith for many intricate mechanisms of social order today. This is the Durkheimian totem, albeit a twisted one, as it has a form of digital infrastructure and not a symbolic centre. Like the Durkheimian counterpart (Durkheim, 2008), cybersecurity is both visible, when it acts, and invisible, when it is feared by the laypeople as the source of social control. Its everyday intricacies are hidden from outsiders but justified in the political arena in terms of theology, mysticism and dangers from uncountable devils. Science, but justified and used for social control as a religion. Unknowable, unable to verify, unaccountable. Exact, palpable and ubiquitous, but only as source of fear and never when it comes to accountability.

A third recognition comes from the fact that queer, alternative, resistant and many other perspectives that challenge the power elites are constantly growing. Czochralski process residues, human and otherwise, are created in every semiconductor factory, during every break of maintenance crew and in every line in infrastructures. With every victim, every unemployed, every victim of surveillance, some knowledge of stabilised instabilities gets disseminated.

There is no other field of knowledge that knows better than cybersecurity that there is no way to show that a system is completely safe. In epistemology, there is no certain way of knowing if one is right, because the problem of induction or experiments' regress will bite back, one way or another. In Christian theology, interaction with this doubt was called a "dark night of the soul", and through the ages, it was associated with all sorts of religious mysticism, direct epistemic connection and even erotic, subliminal sensation.

In a lab, it is called Tuesday.

## Note

1 On an academic note, I wish to pay my utmost professional respects for their multi-site and intersectional work to Stephanie Wuschitz, Eni Maryani, Preciosa Alnashava Janitra, Reksa Anggia Ratmita, Christina Dunbar-Hester and numerous other feminist and/or queer ethnographers of hacking and cybersecurity. The same applies to organisers, activists and all cybersecurity researchers who made this chapter not only possible but impossible to omit.

# Bibliography


Abbott, A. D. (1988). *The system of professions: An essay on the division of expert labor*. University of Chicago Press.

Abu-Ghazaleh, N., Ponomarev, D., & Evtyushkin, D. (2019). How the spectre and meltdown hacks really worked. *IEEE Spectrum*, 56(3), 42–49. https://doi.org/10.1109/MSPEC.2019.8651934

Adams, A. A., Ben-Youssef, F., Schneier, B., & Murata, K. (2020). Superheroes on screen: Real life lessons for security debates. *Security Journal*, 33(4), 565–582. https://doi.org/10.1057/s41284-019-00193-7

Alaimo, S. (2012). States of suspension: Trans-corporeality at sea. *Interdisciplinary Studies in Literature and Environment*, 19(3), Article 3.

Albright, T. D., Baltimore, D., Mazza, A.-M., Mnookin, J. L., & Tatel, D. S. (2023). Science, evidence, law, and justice. *Proceedings of the National Academy of Sciences*, 120(41), e2312529120. https://doi.org/10.1073/pnas.2312529120

Armstrong, N. (2021, wrzesień 17). *A call for feminist analysis in cybersecurity: Highlighting the relevance of the Women, Peace and Security agenda*. LSE Women, Peace and Security Blog. https://blogs.lse.ac.uk/wps/2021/09/17/a-call-for-feminist-analysis-in-cybersecurity-highlighting-the-relevance-of-the-women-peace-and-security-agenda/

Aue, L. (2021). How do metrics shape polities? From analogue to digital measurement regimes in international health politics. *International Political Sociology*, 15(1), 83–101. https://doi.org/10.1093/ips/olaa018

Barbrook, R., & Cameron, A. (1996). The Californian ideology. *Science as Culture*, 6(1), 44–72. https://doi.org/10.1080/09505439609526455

Basu, S., & Biddolph, C. (2025). Queering cybersecurity: An alternative research agenda. *Critical Studies on Security*, 0(0), 1–25. https://doi.org/10.1080/21624887.2025.2502716

Bateson, G. (2000). *Steps to an ecology of mind* (University of Chicago Press ed.). University of Chicago Press.

Bauman, Z. (1988). Is there a postmodern sociology? *Theory, Culture & Society*, 5(2–3), 217–237. https://doi.org/10.1177/026327648800502002

Bellanova, R., & de Goede, M. (2022). The algorithmic regulation of security: An infrastructural perspective. *Regulation & Governance*, 16(1), 102–118. https://doi.org/10.1111/rego.12338

Bellanova, R., Jacobsen, K. L., & Monsees, L. (2020). Taking the trouble: Science, technology and security studies. *Critical Studies on Security*, 8(2), 87–100. https://doi.org/10.1080/21624887.2020.1839852

Bengtsson Meuller, E. (2023). *A feminist theorisation of cybersecurity to identify and tackle online extremism*. King's College London. https://doi.org/10.18742/PUB01-132

Birnhack, M. D., & Mundlak, G. (2025). The Brussels effect(s) and the rise of a privacy profession. *International Data Privacy Law*, ipaf005. https://doi.org/10.1093/idpl/ipaf005

Boltanski, L., & Chiapello, È. (2007). *The new spirit of capitalism*. Verso.

Bowker, G. C., & Star, S. L. (2008). *Sorting things out: Classification and its consequences* (1. paperback ed., 8. print). MIT Press.

Bradford, A. (2021). *The Brussels effect: How the European Union rules the world* (First issued as an Oxford University Press paperback). Oxford University Press.

Bucciarelli, L. L. (1996). *Designing engineers* (First MIT paperback ed.). MIT Press.

Bui, L. T. (2015). Sex hacker: Configuring Chinese women in the age of digital penetration. *Ada: A Journal of Gender, New Media, and Technology*, 6.

Burek, A., Foster, E. A., Fox, S., & Rosner, D. K. (2018). Feminist hackerspaces: Hacking culture, not devices (the zine!). In W J. Sayers (Red.), *Making things and drawing boundaries: Experiments in the digital humanities* (s. 448). University of Minnesota Press.

Butler, J. (2015). *Gender trouble: Feminism and the subversion of identity* (First issued in hardback). Routledge, Taylor & Francis Group.

Cartwright, N. (1983). *How the laws of physics lie* (1. ed.). Oxford University Press. https://doi.org/10.1093/0198247044.001.0001

Cartwright, N. (1991). Replicability, reproducibility, and robustness: Comments on Harry Collins. *History of Political Economy*, 23(1), 143–155. https://doi.org/10.1215/00182702-23-1-143

CERT Polska. (2023). *Krajobraz Bezpieczeństwa Polskiego Internetu w 2022 Roku*. CERT Polska. https://cert.pl/uploads/docs/Raport_CP_2022.pdf.

Chaari, Mohamed Zied, Al-Rahimi, Rashid, Abdelfatah, Mohamed, & Saleh Khamis, Abdulrahman. (2020). Use of reverse engineering method for respirator devices in COVID-19 crisis. In *2020 2nd international conference on electrical, control and instrumentation engineering (ICECIE)* (pp. 1–4). IEEE. https://doi.org/10.1109/ICECIE50279.2020.9309686.

Chałupnik, A. (2023). *Tango jako maszyna pamięci*. Gazeta Teatralna, 175/176. https://didaskalia.pl/pl/artykul/tango-jako-maszyna-pamieci

Chen, C. (2022). *Work pray code: When work becomes religion in Silicon Valley*. Princeton University Press.

clearbluejar. (2023, September 23). *CVE north stars*. Clearbluejar. https://clearbluejar.github.io/

Coleman, G. (2015). The anthropological trickster. *HAU: Journal of Ethnographic Theory*, 5(2), Article 2. https://doi.org/10.14318/hau5.2.024

Coleman, G., & Jandrić, P. (2019). Postdigital anthropology: Hacks, hackers, and the human condition. *Postdigital Science and Education*, 1(2), 525–550. https://doi.org/10.1007/s42438-019-00065-8

Coleman, G. E. (2010). The hacker conference: A ritual condensation and celebration of a lifeworld. *Anthropological Quarterly*, 83(1), Article 1.

Coleman, G. E. (2013). *Coding freedom: The ethics and aesthetics of hacking*. Princeton University Press. https://doi.org/10.1515/9781400845293

Collins, H. (2013). *Tacit and explicit knowledge*. University of Chicago Press.

Collins, H. (2017). *Gravity's kiss: The detection of gravitational waves*. The MIT Press.

Collins, H. (2019). *Forms of life: The method and meaning of sociology*. The MIT Press.

Collins, H., & Evans, R. (2009). *Rethinking expertise* (Paperback ed.). University of Chicago Press.

Collins, P. H., Da Silva, E. C. G., Ergun, E., Furseth, I., Bond, K. D., & Martínez-Palacios, J. (2021). Intersectionality as critical social theory: Intersectionality as critical social theory, Patricia Hill Collins, Duke University Press, 2019. *Contemporary Political Theory*, 20(3), 690–725. https://doi.org/10.1057/s41296-021-00490-0

crimew arson, maia. (2024, lipiec 28). *OPINION: Stop studying cybersecurity because of me. Im trying to get u into activism, not college*. Maia Blog. https://maia.crimew.gay/posts/please/#jackie-singh-note

Cukier, K., & Mayer-Schoenberger, V. (2013). The rise of big data: How it's changing the way we think about the world. *Foreign Affairs*, 92(3), 28–40.

Dennett, D. C. (2013). *Intuition pumps and other tools for thinking* (1. ed.). W. W. Norton & Company.

Dian, D. (2024). Lala activists in dark times: Queer feminist resistance to the cyber-nationalist attacks in China. *Journal of Lesbian Studies*, 28(3), 460–485. https://doi.org/10.1080/10894160.2023.2281060

Doing, P. (2009). *Velvet revolution at the synchrotron: Biology, physics, and change in science*. MIT Press.

drbix. (2021). *Modify in-flight data to payment provider Smart2Pay*. HackerOne. https://hackerone.com/reports/1295844.

Dunbar-Hester, C. (2019). Hacking diversity: The politics of inclusion in open technology cultures. In *Hacking diversity*. Princeton University Press. https://doi.org/10.1515/9780691194172

Durkheim, É. (2008). *The elementary forms of religious life* (C. Cosman & M. S. Cladis, Trans.). Oxford University Press.

Edwards, B., Jacobs, J., & Forrest, S. (2019). Risky business: Assessing security with external measurements (arXiv:1904.11052). *arXiv*. https://doi.org/10.48550/arXiv.1904.11052

Egher, C. (2020). Online expert mediators: The rise of a new 'bipolar' stakeholder or going beyond interactional expertise in the blogosphere. *Science & Technology Studies*, 33(2), Article 2. https://doi.org/10.23987/sts.60782

ENISA. (2025, May 14). *European Union vulnerability database*. https://euvd.enisa.europa.eu/

Eren, E. (2022). Talking science and feminism. *Journal of Gender Studies*, 31(8), 911–927. https://doi.org/10.1080/09589236.2022.2091527

Eskhita, R., & Stamhuis, E. (2024). *The influence of the Brussels effect on the interpretation of data protection laws in the Gulf*. https://doi.org/10.1163/2211906X-13020007

Feenberg, A. (2015). Lukács's theory of reification and contemporary social movements. *Rethinking Marxism*, 27(4), 490–507. https://doi.org/10.1080/08935696.2015.1076968

Fleck, Ludwik. (2008). *Genesis and development of a scientific fact*. Repr. 11. Aufl. Sociology of Science. University of Chicago Press.

Fox, S., Ulgado, R. R., & Rosner, D. (2015). Hacking culture, not devices: access and recognition in feminist hackerspaces. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, 56–68. https://doi.org/10.1145/2675133.2675223

Galison, P. (1994). The ontology of the enemy: Norbert Wiener and the cybernetic vision. *Critical Inquiry*, 21(1), 228–266. https://doi.org/10.1086/448747

Galison, P. (1997). *Image and logic: A material culture of microphysics*. University of Chicago Press.

Galison, P. (2010). Trading with the enemy. In M. E. Gorman (Ed.), *Trading zones and interactional expertise: Creating new kinds of collaboration* (p. 302). MIT Press.

Gebru, T., & Torres, É. P. (2024). The TESCREAL bundle: Eugenics and the promise of utopia through artificial general intelligence. *First Monday*. https://doi.org/10.5210/fm.v29i4.13636

Georgoulias, D., Yaben, R., & Vasilomanolakis, E. (2023). Cheaper than you thought? A dive into the darkweb market of cyber-crime products. *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 1–10. https://doi.org/10.1145/3600160.3605012

Gorman, M. E. (Ed.). (2010). *Trading zones and interactional expertise: Creating new kinds of collaboration*. MIT Press.

Gramsci, A. (2007). *Selections from the prison notebooks of Antonio Gramsci* (Q. Hoare & G. Nowell-Smith, Eds.; Reprinted). Lawrence and Wishart.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state* (1. ed.). Metropolitan Books/Henry Holt.

Hacking, I. (2001). *The social construction of what?* (7. print). Harvard University Press.

Hamer, J. M. M., Kemp, P. E. J., Wong, B., & Copsey-Blake, M. (2023). Who wants to be a computer scientist? The computing aspirations of students in English secondary schools. *International Journal of Science Education*, 45(12), 990–1007. https://doi.org/10.1080/09500693.2023.2179379

Haraway, D. (2006). A cyborg manifesto: Science, technology, and socialist-feminism in the late twentieth century. In *The transgender studies reader*. Routledge.

Harris, M. (with Little, Brown and Company). (2023). *Palo Alto: A history of California, capitalism, and the world* (1. ed.). Little, Brown and Company.

Hayles, N. K. (2006). Unfinished work: From cyborg to cognisphere. *Theory, Culture & Society*, 23(7–8), 159–166. https://doi.org/10.1177/0263276406069229

Henke, C., & Sims, B. (2020). *Repairing infrastructures: The maintenance of materiality and power*. The MIT Press.

Herley, C., & Van Oorschot, P. C. (2017). SoK: Science, security and the elusive goal of security as a scientific pursuit. *2017 IEEE Symposium on Security and Privacy (SP)*, 99–120. https://doi.org/10.1109/SP.2017.38

Hermanowicz, J. C. (2009). *Lives in science: How institutions affect academic careers*. University of Chicago press.

Hesmondhalgh, D. (2021). The infrastructural turn in media and internet research. In *The Routledge companion to media industries*. Routledge.

Hunsinger, J., & Schrock, A. (2016). The democratization of hacking and making. *New Media & Society*, 18(4), 535–538. https://doi.org/10.1177/1461444816629466

Hutchins, Edwin. (1996). *Cognition in the wild* (2. print). A Bradford Book. MIT Press.

Jasanoff, Sheila. (2015). Future imperfect: Science, technology, and the imaginations of modernity. In Sheila Jasanoff & Sang-Hyun Kim (Eds.), *Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power* (p. 0). University of Chicago Press. https://doi.org/10.7208/chicago/9780226276663.003.0001.

JASON. (2010). *Science of cyber-security*. JASON Office MITRE.

Jones, M. L., & Levendowski, A. M. (Red.). (2024). *Feminist cyberlaw*. University of California Press.

Kaiser, D. (Ed.). (2005). *Pedagogy and the practice of science: Historical and contemporary perspectives*. MIT Press.

Kalmar, I. D. (2022). *White but not quite: Central Europe's illiberal revolt*. Bristol University Press.

Kappa. (2025). FBI most wanted girlfriend: The futurist model of fugitive trans hacker and merchandiser Maia Arson Crimew's meaning Makin. In W. S. J. Blackmon & S. Karahan (Red.), *Proceedings of the 20th international conference on cyber warfare and security* (T. 20). Academic Conferences International Limited.

Kelty, C. M. (2008). *Two bits: The cultural significance of free software*. Duke University Press. https://doi.org/10.1215/9780822389002

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking humans? Social engineering and the construction of the "Deficient User" in cybersecurity discourses. *Science, Technology, & Human Values*, 46(6), Article 6. https://doi.org/10.1177/0162243921992844

Knorr-Cetina, K. (1999). *Epistemic cultures: How the sciences make knowledge*. Harvard University Press.

Kowalczyk, M., q3k, & Stepniewicz, J. (2025, December 27). *We've not been trained for this: Life after the Newag DRM disclosure*. 38C3, Hamburg. https://media.ccc.de/v/38c3-we-ve-not-been-trained-for-this-life-after-the-newag-drm-disclosure

Kubitschko, S. (2015). Hackers' media practices: Demonstrating and articulating expertise as interlocking arrangements. *Convergence: The International Journal of Research into New Media Technologies*, 21(3), Article 3. https://doi.org/10.1177/1354856515579847

Lampland, M., & Star, S. L. (Eds.). (2009). *Standards and their stories: How quantifying, classifying, and formalizing practices shape everyday life*. Cornell University Press.

Latour, B. (2000). *Pandora's hope: Essays on the reality of science studies* (2. print). Harvard University Press.

Larkin, B. (2013). The politics and poetics of infrastructure. *Annual Review of Anthropology*, 42(1), 327–343. https://doi.org/10.1146/annurev-anthro-092412-155522

Latour, B. (2012). Visualisation and cognition: Drawing things together. *Avant: Trends in Interdisciplinary Studies*, 3(T), 207–260.

Latour, B., & Woolgar, S. (1986). *Laboratory life: The construction of scientific facts*. Princeton University Press.

Lee, C. P., & Schmidt, K. (2018). A bridge too far? Critical remarks on the concept of "Infrastructure" in computer-supported cooperative work and information systems. In V. Wulf, V. Pipek, D. Randall, M. Rohde, K. Schmidt, & G. Stevens (Eds.), *Socio-Informatics* (p. 0). Oxford University Press. https://doi.org/10.1093/oso/9780198733249.003.0006

Lemnitzer, J. M. (2021). Why cybersecurity insurance should be regulated and compulsory. *Journal of Cyber Policy*, 6(2), 118–136. https://doi.org/10.1080/23738871.2021.1880609

Levendowski, A. (2022). Defragging feminist cyberlaw. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4208296

Lindtner, S. (2015). Hacking with Chinese characteristics: The promises of the maker movement against China's manufacturing culture. *Science, Technology, & Human Values*, 40(5), 854–879. https://doi.org/10.1177/0162243915590861

Machalewski, T. K., Szymanek, M. H., Czubak, A., & Turba, T. (2024). Expressing impact of vulnerabilities: An expert-filled dataset and vector changer framework for modelling multistage attacks, based on CVE, CVSS and CWE. In D. Grzonka, N. Rylko, G. Suchacka, & V. Mityushev (Eds.), *Proceedings of the 38th ECMS international conference on modelling and simulation ECMS 2024* (Vol. 38). European Council for Modelling and Simulation.

Marcus, G. E. (1995). Ethnography in/of the world system: The emergence of multi-sited ethnography. *Annual Review of Anthropology*, 24, 95–117.

Marczak, B., Scott-Railton, J., McKune, S., Bahr Razzak, A., & Deibert, R. (2018). *Hide and seek*. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries (Citizen Lab Research Report No. 113). University of Toronto. Citizen Lab.

Margolis, J., & Fisher, A. (2003). *Unlocking the clubhouse: Women in computing* (1. paperpack ed.). MIT Press.

Marx, K. (2024). *Capital: A critique of political economy* (Vol. 1). Princeton University Press.

Mauro, A. (2022). *Hacking in the humanities: Cybersecurity, speculative fiction, and navigating a digital future*. Bloomsbury Academic.

Mazur, J., & Włoch, R. (2023). Embedding digital economy: Fictitious triple movement in the European Union's Artificial Intelligence Act. *Social & Legal Studies*, 09646639231152866. https://doi.org/10.1177/09646639231152866

Messias, E., Gathright, M. M., Freeman, E. S., Flynn, V., Atkinson, T., Thrush, C. R., Clardy, J. A., & Thapa, P. (2019). Differences in burnout prevalence between clinical professionals and biomedical scientists in an academic medical centre: A cross-sectional survey. *BMJ Open*, 9(2), e023506. https://doi.org/10.1136/bmjopen-2018-023506

Mhajne, A., & Henshaw, A. (2024). *Critical perspectives on cybersecurity: Feminist and postcolonial interventions*. Oxford University Press.

Mhajne, A., & Whetstone, C. (2024). A feminist cybersecurity: Addressing the crisis of cyber(in)security. *International Affairs*, 100(6), 2341–2360. https://doi.org/10.1093/ia/iiae234

Mhajne, A., & Whetstone, C. (2025). *32: Redefining (in-)security in cybersecurity: An intersectional lens*. https://www.elgaronline.com/edcollchap/book/9781803928364/chapter32.xml

Mildebrath, H. (2022). *Europe's PegasusGate* (p. 122). Secretariat of the European Parliament.

Mills, C. W. (2000a). *The sociological imagination* (40. anniversary ed.). Oxford University Press.

Mills, C. W. (with Wolfe, A.). (2000b). *The power elite* (2. ed.). Oxford University Press.

Mirowski, P. (2011). *Science-mart: Privatizing American science*. Harvard University Press.

Mirowski, P. (2018). The future(s) of open science. *Social Studies of Science*, 48(2), 171–203. https://doi.org/10.1177/0306312718772086

MITRE. (2023). *CVE-2023-23397*. https://www.cve.org/CVERecord?id=CVE-2023-23397

Mol, A. (2002). *The body multiple: Ontology in medical practice*. Duke University Press. https://doi.org/10.1215/9780822384151

Mößner, Nicola. (2011). Thought styles and paradigms—a comparative study of Ludwik Fleck and Thomas S. Kuhn. *Studies in History and Philosophy of Science Part A, Model-Based Representation in Scientific Practice*, 42(2), 362–371. https://doi.org/10.1016/j.shpsa.2010.12.002.

Moura, G. C. M., & Heidemann, J. (2023). Vulnerability disclosure considered stressful. *ACM SIGCOMM Computer Communication Review*, 53(2), 2–10. https://doi.org/10.1145/3610381.3610383

Msambwa, M. M., Daniel, K., Lianyu, C., & Antony, F. (2025). A systematic review using feminist perspectives on the factors affecting girls' participation in STEM subjects. *Science & Education*, 34(3), 1619–1650. https://doi.org/10.1007/s11191-024-00524-0

Muntanyola-Saura, D. (2022). Habitus in dance: The social and artistic skills of a rehearsal. In A. Rodríguez Morató & A. Santana-Acuña (Eds.), *Sociology of the arts in action: New perspectives on creation, production, and reception* (pp. 143–164). Springer International Publishing. https://doi.org/10.1007/978-3-031-11305-5_6

Nijakowski, L. M. (2019). *Świat po apokalipsie: Społeczeństwo w świetle postapokaliptycznych tekstów kultury popularnej (Wydanie drugie)*. Wydawnictwo Naukowe Scholar.

NIST. (2023). *NVD - cve-2023-23397*. https://nvd.nist.gov/vuln/detail/cve-2023-23397

Noble, D. F. (1997). *The religion of technology: The divinity of man and the spirit of invention*. Random House.

Noble, D. F. (2011). *Forces of production: A social history of industrial automation*. Transaction Publishers.

Nowak, A. W. (2016). *Wyobraźnia ontologiczna: Filozoficzna (re)konstrukcja fronetycznych nauk społecznych*. Wydawnictwo Naukowe Uniwerstetu im. Adama Mickiewicza ; Instytut Badań Literackich PAN Wydawnictwo.

Oreskes, N. (2021). *Science on a mission: How military funding shaped what we do and don't know about the ocean*. University of Chicago Press.

Orr, J. E. (1996). *Talking about machines: An ethnography of a modern job*. ILR Press.

Pasquinelli, M. (2023). *The eye of the master: A social history of artificial intelligence*. Verso.

Polanyi, Michael. (2009). *The tacit dimension*. University of Chicago Press.

Popper, K. (2010). *The logic of scientific discovery* (Special Indian ed.). Routledge.

Poster, W. R. (2026). *Multi-surveillances: Transnational digital agencies in the outsourced services of Indian call centers*. MIT Press.

Powell, A. (2016). Hacking in the public interest: Authority, legitimacy, means, and ends. *New Media & Society*, 18(4), 600–616. https://doi.org/10.1177/1461444816629470

Price, D. J. de S. (1971). *Little science, big science*. Columbia University Press.

Prout, A., Arcand, W., Bestor, D., Bergeron, B., Byun, C., Gadepally, V., Houle, M., Hubbell, M., Jones, M., Klein, A., Michaleas, P., Milechin, L., Mullen, J., Rosa, A., Samsi, S., Yee, C., Reuther, A., & Kepner, J. (2018). Measuring the impact of spectre and meltdown. *2018 IEEE High Performance Extreme Computing Conference (HPEC)*, 1–5. https://doi.org/10.1109/HPEC.2018.8547554

q3k, (@q3k@hackerspace.pl). (2023). *"The key unlock was deleted in newer PLC software versions, but the lock logic remained. After a certain update by NEWAG, the cabin controls . . .." Mastodon post*. Mastodon. https://social.hackerspace.pl/@q3k/111528169261508544.

*Raport końcowy z prac Komisji Nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych* (X Kadencja Senatu, p. 58). (2023). [Parliamentary Investigative Committee Final Report]. Senat Rzeczypospolitej Polskiej. https://www.senat.gov.pl/aktualnoscilista/art,15764,komisja-nadzwyczajna-ds-inwigilacji-przyjela-raport-ze-swoich-prac.html

Redford, q3k, & MrTick. (2023). *Breaking "DRM" in Polish trains*. 37C3, Hamburg. https://media.ccc.de/v/37c3-12142-breaking_drm_in_polish_trains

Richard, L., & Rigaud, S. (2024). *Pegasus*. Holt Paperback.

Rider, K., & Murakami Wood, D. (2019). Condemned to connection? Network communitarianism in Mark Zuckerberg's "Facebook Manifesto". *New Media & Society*, 21(3), 639–654. https://doi.org/10.1177/1461444818804772

Rommetveit, K., & van Dijk, N. (2022). Privacy engineering and the techno-regulatory imaginary. *Social Studies of Science*, 52(6), Article 6. https://doi.org/10.1177/03063127221119424

Rosenthal, C. (2019). *Accounting for slavery: Masters and management* (First Harvard University Press paperback printing). Harvard University Press.

Rosinska, A., & Pellerito, E. (2023). Advocating for survival: Domestic workers in the necropolitical regime of the pandemic. *Social Politics: International Studies in Gender, State & Society*, 30(4), 1064–1088. https://doi.org/10.1093/sp/jxad025

Rouhana, N. N., & Šalhūb-Kīfūrkiyān, N. (Red.). (2021). *When politics are sacralized: Comparative perspectives on religious claims and nationalism*. Cambridge University Press.

Sady, Wojciech. (2023, Fall). Ludwik Fleck. In Edward N. Zalta & Uri Nodelman (Eds.), *The Stanford encyclopedia of philosophy*. Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/fall2023/entries/fleck/.

Šalhūb-Kīfūrkiyān, N. (2015). *Security theology, surveillance and the politics of fear*. Cambridge University Press.

Sandvig, C. (2013). *The Internet as Infrastructure* (W. H. Dutton, Ed.; Vol. 1). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199589074.013.0005

Schneier, B. (2009). *Beyond security theater*. Schneier on Security. https://www.schneier.com/essays/archives/2009/11/beyond_security_thea.html

Serwis RP. (2019). *Narodowe standardy Cyberbezpieczeństwa*. Baza wiedzy. https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber

Shapin, S., & Schaffer, S. (1985). *Leviathan and the air-pump: Hobbes, Boyle, and the experimental life*. Princeton university press.

Shires, James. (2020). Cyber-noir: Cybersecurity and popular culture. *Contemporary Security Policy*, 41(1), 82–107. https://doi.org/10.1080/13523260.2019.1670006.

Sitarczyk, J. (2025, May 13). *Przeczytałem NIST CSF, abyście Wy nie musieli*. White Hats. https://whitehats.pwr.edu.pl/research/nist-cfs/

SKW. (2025). *Działania rosyjskiej służby GRU wymierzone w zachodnie podmioty logistyczne oraz przedsiębiorstwa technologiczne. Służba Kontrwywiadu Wojskowego*. https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-0530.pdf

Śledziewska, K., & Włoch, R. (2021). *The economics of digital transformation: The disruption of markets, production, consumption and work*. Routledge.

Slupska, J. (2019). Safe at home: Towards a feminist critique of cybersecurity. *St Antony's International Review*, 15(1), 83–100.

Söderberg, J., & Delfanti, A. (2015). Hacking hacked! The life cycles of digital innovation. *Science, Technology, & Human Values*, 40(5), 793–798. https://doi.org/10.1177/0162243915595091

Söderberg, J., & Maxigas, M. (2022). *Resistance to the current: The dialectics of hacking*. https://doi.org/10.7551/mitpress/13466.001.0001

Spring, J. M. (2023). An analysis of how many undiscovered vulnerabilities remain in information systems. *Computers & Security*, 131, 103191. https://doi.org/10.1016/j.cose.2023.103191

Spring, J. M., & Illari, P. (2019). Building general knowledge of mechanisms in information security. *Philosophy & Technology*, 32(4), 627–659. https://doi.org/10.1007/s13347-018-0329-z

Spring, J. M., & Illari, P. (2025). Information security, intelligence analysis, and knowledge generation without experiments. In P. Illari & F. Russo (Eds.), *The Routledge handbook of causality and causal methods*. Routledge, Taylor & Francis Group.

Spring, J. M., Moore, T., & Pym, D. (2017). Practicing a science of security: A philosophy of science perspective. *Proceedings of the 2017 New Security Paradigms Workshop*, 1–18. https://doi.org/10.1145/3171533.3171540

Star, S. L. (1990). Power, technology and the phenomenology of conventions: On being allergic to onions. *The Sociological Review*, 38(1_suppl), Article 1_suppl. https://doi.org/10.1111/j.1467-954X.1990.tb03347.x

Star, S. L. (1999). The ethnography of infrastructure. *American Behavioral Scientist*, 43(3), 377–391. https://doi.org/10.1177/00027649921955326

Star, S. L., & Griesemer, J. R. (1989). Institutional Ecology, 'Translations' and boundary objects: Amateurs and professionals in Berkeley's Museum of Vertebrate Zoology, 1907–39. *Social Studies of Science*, 19(3), 387–420. https://doi.org/10.1177/030631289019003001

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research*, 7(1), 111–134. https://doi.org/10.1287/isre.7.1.111

Thubron, Rob. (2021). *Valve pays researcher $7,500 for discovering exploit that could add unlimited funds to steam wallets*. Techspot.

Toh, L., & Watt, H. M. G. (2022). How do adolescent mathematical self-concept and values explain attainment of different kinds of STEM degrees in adulthood? *Contemporary Educational Psychology*, 69, 102057. https://doi.org/10.1016/j.cedpsych.2022.102057

Traweek, S. (1992). *Beamtimes and lifetimes: The world of high energy physicists* (1. ed.). Harvard University Press.

Turkle, S. (2005). *The second self: Computers and the human spirit*. The MIT Press. https://doi.org/10.7551/mitpress/6115.001.0001

Turner, V. (1995). *The anthropology of performance* (Nachdr.). PAJ Publishing.

Turner, V. (2008). *From ritual to theatre: The human seriousness of play* (6. print). PAJ Publishing.

van Gennep, A. (2019). *The rites of passage* (M. B. Vizedom & G. L. Caffee, Trans.; 2. ed.). The University of Chicago Press.

Varoufakis, Y. (2023). *Technofeudalism: What killed capitalism*. The Bodley Head.

Veldman, J., Van Laar, C., Thoman, D. B., & Van Soom, C. (2021). "Where will I belong more?": The role of belonging comparisons between STEM fields in high school girls' STEM interest. *Social Psychology of Education*, 24(5), 1363–1387. https://doi.org/10.1007/s11218-021-09663-6

Vertesi, J. (2015). *Seeing like a Rover: How robots, teams, and images craft knowledge of Mars*. The University of Chicago Press.

Voß, J.-P., Schritt, J., & Sayman, V. (2022). Politics at a distance: Infrastructuring knowledge flows for democratic innovation. *Social Studies of Science*, 52(1), Article 1. https://doi.org/10.1177/03063127211033990

Wagner, I. (2011). *Becoming transnational professional: Kariery i mobilność polskich elit naukowych*. Wydawnictwo Naukowe Scholar.

Well, L., Currie, M., & Stewart, J. (2023). Surveillance, discretion and governance in automated welfare: The case of the German ALLEGRO system. *Science & Technology Studies*, 36(1), Article 1. https://doi.org/10.23987/sts.100490

West, S. M. (2022). Cryptography as information control. *Social Studies of Science*, 52(3), Article 3. https://doi.org/10.1177/03063127221078314

Whittaker, M. (2023). Origin stories: Plantations, computers, and industrial control. *Logic(s)*, 19. https://logicmag.io/supa-dupa-skies/origin-stories-plantations-computers-and-industrial-control/

Wolfe, A. J. (2020). *Freedom's laboratory: The Cold War struggle for the soul of science* (Johns Hopkins paperback ed.). Johns Hopkins University Press.

Wong, B. (2016). 'I'm good, but not that good': Digitally-skilled young people's identity in computing. *Computer Science Education*, 26(4), 299–317. https://doi.org/10.1080/08993408.2017.1292604

Wong, B., Hamer, J. M. M., Copsey-Blake, M., & Kemp, P. E. J. (2024). Is being clever enough? Young people's construction of the ideal student in computer science education. *Educational Review*, 0(0), 1–20. https://doi.org/10.1080/00131911.2024.2379430

Wuschitz, S., & Reza, A. (2021). Coded feminisms in Indonesia. Electronic workshops in computing. *Proceedings of Politics of the Machines - Rogue Research 2021*. https://doi.org/10.14236/ewic/pom2021.31

Xu, M., & Hua, L. (2019). Cybersecurity insurance: Modeling and pricing. *North American Actuarial Journal*, 23(2), 220–249. https://doi.org/10.1080/10920277.2019.1566076

Ylönen, M. (2025). Reconceptualising the Brussels effect. *JCMS: Journal of Common Market Studies*. https://doi.org/10.1111/jcms.13731

Zaród, M. (2018). *Aktorzy-sieci w kolektywach hakerskich*. https://depotuw.ceon.pl/handle/item/2909

Zaród, M. (2021). Tools of the game. Qualitative digital methodologies for the e-sports research. *Przegląd Socjologii Jakościowej*, 17(1), 26–40.

Zaród, M. (2022). When social theory is devoid of social history. Reply to "Transhumanism. Human Nature and Culture: A Preliminary Sociological Contextualization" by Markus Lipowicz. *Studia Socjologiczne*, 4(247), 173–183. https://doi.org/10.24425/sts.2022.143587

Zaród, M., Wadowski, J., & Kostyszak, M. (2015). Engineering education in Slavic languages countries. In B. Newberry, C. Mitcham, M. Meganck, A. Jamison, C. Didier, & S. H. Christensen (Eds.), *International perspectives on engineering education: Engineering education and practice in context*. Springer Verlag.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (1. ed.). PublicAffairs.

Zuboff, S. (2022). The EU has fired the starting gun in the fightback against Big Tech. *Financial Times*.

# Index

Page numbers followed by n denote notes.