# Ethical dilemmas in strategical and operational cybersecurity at State level

The CANVAS Project*

2019/05/13-14

**Abstract**

Our international workshop on "Ethical dilemmas in strategical and operational cybersecurity at State level" in Lausanne, Switzerland will begin with a focus on ethical issues in day-to-day operations for penetration testers, operators of critical infrastructure, and CERTs providing technical reaction to threats. Towards the end, we will broaden the scope to furthermore look at value-driven creation of new regulations and standards.

## 1 May 13th: Ethical dilemmas for pen-testers and operators of critical infrastructure.

### 1.1 9:00: David-Olivier Jaquet-Chiffelle and Olivier Ribaux (ESC, University of Lausanne) — Welcome

This presentation will give a brief overview over the CANVAS project and the workshop in particular.

### 1.2 9:30: Melanie Rieback (Radically Open Security) — Ethics and Pentesting

Pentesting is a minefield of ethical issues. Whether in a commercial or open-source setting, there's daily decisions to be made about process and tooling, (responsible) disclosure, pentest scoping, phishing pretexts, etc.. This necessitates active discussion, and pursuit of a culture of ethical awareness and inquiry.

*This international and interdisciplinary workshop is part of a series of events organized by the Horizon 2020 project CANVAS. The goal of CANVAS is to inform deciders and policy makers about issues at the intersection of ethics and cybersecurity by creating briefing packages, whitepapers, and materials for teaching (MOOC, reference curriculum, and a book). Our event brings together scholars and practitioners. This includes actors who need protection for themselves or for their organization as well as those who have to deal with the consequences of untraceability and online anonymity.

In this presentation, Melanie Rieback shares her experiences at Radically Open Security (ROS) and discusses how ROS navigates through this minefield.

### 1.3 10:15: Benjamin Kunz Mejri (Evolution Security) — Intelligence Vulnerability Management, Databases & Models

1. International vulnerability databases
   - Models
   - Coordination
   - Researchers
   - Needs behind the build
2. Protection of databases against public abuse
   - APTs
   - Cyber criminals
3. Social benefit of vulnerability databases
   - Public Folks
   - Institutions
   - Governments Sector
   - Military Sector
4. CVE System insufficient & why
   - Centralized System
   - Decentralized Systems
5. What brings the future of Vulnerability Databases?

### 1.4 11:15: Stephane Bortzmeyer (AFNIC) – Rendez-vous techniques: the weakest link? The example of the DNS.

In computer networks, even when Alice can talk directly to Bob, there is often an intermediate step: a rendez-vous technique that will tell Alice where in the network to find Bob. If this step fails, Alice can no longer talk to Bob. If this step is malicious, Alice may be redirected to Mallory instead of Bob. On the Internet, this rendez-vous technique is almost always the Domain Name System (DNS). The DNS is both crucial and often forgotten or misunderstood. Nevertheless, some people are well aware of its critical character and tries to use it for their own goals. For instance, it is common to use the DNS as a control point, and not as a service. Asking the operators to modify the DNS answers is used for

state censorship, as well as for other types of control. What is the extent of this control? Who are the actors and what are their respective interests? What the users can do to reclaim some neutrality from this service? Practically speaking, should we move from the DNS to another system? Or from the DNS as we use it today to a different architecture, for instance by delegating DNS resolution to big actors? We will discuss the consequences of this pressure on the DNS for the network reliability and for the general landscape of the Internet, with the rise of many alternative harder-to-control solutions.

Other problems can arise from this criticality of the Domain Name System. The massive campaign of domain name hijackings by an unknown group of professionnal bad actors at the end of 2018, targeting mostly governments in the Middle-East but also some elements of the more general infrastructure of the Internet, reminded us of the possibility for the attackers to go after the rendez-vous techniques, instead of attacking directly the endpoints. It was not the first time such an attack took place, but it was remarkable by its size. What lessons could be drawn from this campaign? In this specific set of attacks, the attackers wanted (and often succeeded) to take control of some domain names. But sometimes the attackers attempt instead to disrupt the DNS, launching denial-of-service attacks, like the one that targeted the DNS hoster Dyn in 2016.

Because the DNS is not as well-known as some other services on the Internet, this talk will start with a short introduction to domain names and to the DNS protocol.

# 2 May 13th: Ethical dilemmas during technical reaction

## 2.1 13:30: Freddy Dezeure — Ethical challenges in incident response

When carrying out an APT incident response we are confronted with a variety of legal challenges, in addition to the technical ones. Speed of containment and remediation in constituent's infrastructure seem to be the obvious goal. However, lack of access to telemetry data can severely hamper the response. How should the responder react in view of legal and data protection constraints? Break the law in order to resolve the incident and notify victims? And subsequently, which victims should he notify? All of them? Immediately?

## 2.2 14:30: Tomi Tuominen (F-Secure) — Ghost story

Proponents of coordinated disclosure believe that software vendors have the right to control vulnerability information concerning their products. The primary tenet of coordinated disclosure is that nobody should be informed about a vulnerability until the software vendor gives their permission.

Unfortunately, too often vendors are not prepared to receive and handle vulnerability reports from outside parties. As a result, they end up going through Kübler-Ross stages of grief during the process. This in turn can lead to some very unfortunate and uncomfortable situations.

### 2.3 15:00: Reto Inversini and Andreas Greulich (MELANI) — Ethical and legal dilemmata during operations against APT groups

During our speech we present different ethical challenges we experienced during attacks against infrastructures of Switzerland. We are going to discuss different decisions the incident response team had to make und time pressure and which could not be resolved on a purely technical or legal base. We will show that a common set of values shared by all team members is crucially important to find efficient and ethically sound decisions during security incidents.

## 3 May 13th, 16:30: Richard M. Stallman (The GNU Project) — Cyberpeace requires Free Software

Free software (libre, freie) is software that is under the control of the users, both separately and in groups, and therefore respects their freedom and community. There are many ethical reasons to demand that the software you use be free, and cyberpeace is one of them.

A non-free program is under the control of one entity, its developer. As a consequence, you cannot trust it to provide security against all possible attackers: the developer can install a vulnerability to exploit later, and users cannot detect that, let alone fix it.

Only a free program can try to offer security against all possible attackers, including its own contributors, because the users can verify and improve its security.

Cyberimperialist states such as Australia now claim the power to force developers in other countries to install a vulnerability, using threats to extort treachery. The developer of a non-free program cannot cite a real obstacle that would exxcuse not carrying out this treachery. With free software, the community has a chance to protect itself from this.

# 4 May 14th: Protecting values in strategic plans for better cyber security

## 4.1 9:00: Manuel Suter (National Coordination Center, CH) — Building national Cybersecurity Strategies: democratic challenges

In cybersecurity governments depend heavily on the capacities and knowledge of private sector actors. They thus not only work with private actors at the operational level, but also integrate them into the development of national cyber strategies. Such a broad interpretation of a collaborative governance through and with public-private networks is generally perceived as a modern and efficient solution to complex problems. It however rises also questions about the democratic legitimation of these processes and policymakers must carefully consider how the democratic principles of accountability and transparency can be taken into account in processes of joint strategy building.

## 4.2 9:45: Nouschka Auwema (NCSC-NL)

The National Cyber Security Centre of the Netherlands is the national point of contact for Responsible Disclosure/Coordinated Vulnerability Disclosure reports for its own systems and those of Dutch (national) government organisations and those in vital sectors. We receive reports and notifications of vulnerabilities on a daily basis. This presentation will outline what this policy entails, how it can be integrated in incident management and specifically how organisations can improve their own strategic security planning before, during and after such an incident. The focus will be on the technical incident handling as well as on the organisational issues that will arise.

## 4.3 11:00: Juha Röning (University of Oulu) — AI: Is it a fair play on software security?

The National Institute of Standards and Technology plans to move to a vulnerability scoring method that uses IBM's Watson artificial intelligence system by October 2019. So far Watson stumbled when evaluating new and complex vulnerabilities. So AI is sneaking in to cyber security business, but does it make us stronger or more vulnerable.

AI in its recent form and development is a powerful tool but contains some risks and ethical questions we should be aware and consider. We should not just trust learning AI methods like a magic black box. The decision making should be "transparent". We need to understand how it works and have command over it. At the same time our officials main concern is not anymore that hackers will steal data, but that they will change data. This follows that users will unwittingly rely on false information.

Recent terroristic attacks with common tools or equipment have resulted to demands to test products for abusability. Tech firms should foresee the unintended consequence of technology. What about the malicious use of AI.

With this talk I would like to raise the issues, how much one can trust AI-based decisions. What risks of autonomous response actions might have? Double blade of AI i.e. AI arms race between defenders and attackers.

# 5 May 14th: Enforcing the law in cyberspace

## 5.1 13:30: Harald Zwingelberg (ULD Schleswig-Holstein) — Enforcing data protection in cyberspace — Challenges and strategies

Rules and regulations on data protection provide safeguards for fundamental rights - primarily the ones on respect for private and family life and the protection of personal data. This also defines the interest data protection caters for. These interests stand in a potential conflict with those of criminal prosecution and ICT security. In the field of Cybersecurity many measures to ensure ICT security and data protection are identical and this may mislead to the conclusion that security and data protection are two sides of the same medal. In reality inherent conflict lines must to be watched and addressed. While for security the interests of protecting own commercial assets and business secrets tend to match with the ones of the controlling organisation data protection focusses on the concners of data subjects. This also leads to deviating understandings of relevant core terminology such as anonymity and pseudonymity. With a view on services providing anonymity for users and provides of services and goods online this will be exemplified.

## 5.2 14:15: Stephan Walder (Staatsanwaltschaft II des Katons Zürich) — Cybercrime - possibilities and limitations of penal prosecution

First, the term Cybercrime is defined in the form of a “tour d’horizon” and challenged based on recent development of these phenomenons. In the second part, the localization and identification of perpetrators in national and international is presented and discussed.

# 6 May 14th: Approaches for knowledge-based collaborative solutions

## 6.1 15:30: Daniel Plohmann (Fraunhofer FKIE) — 1 + 1 = 3? Experiences with Fostering Collaboration in Cybersecurity

When defending against security threats, many organizations and analysts are confronted with very similar attack patterns. Therefore, collaboration and information sharing are a great way to avoid double efforts and to generally improve security posture. In this presentation we will present our lessons learned while building two community projects: DGArchive and Malpedia. As it is always hard to please everybody in such endeavors, we will especially address some of the ethical and legal challenges encountered along the way.

## 6.2 16:00: Martin Dion (Kudelski Security) — Securing the State & the People in Cyberspace — An ethical dilemma or just a big misunderstanding?

Over the past three decades, cyberspace and the use of technology have profoundly impacted our modern society and economy. Almost everybody became either an Information Technology specialist to some extent or a heavy consumer of online services and connected technologies in both their personal and professional life. Given those societal changes, one should not be surprised that the darker side of human behaviours also crept into the digital terrain. But did our political institutions and we, as a society, evolved accordingly when it comes to the security and safety of the people and our industries in cyberspace? On the one hand, the people want full liberty, privacy and even anonymity in cyberspace and at the same time, are expecting security and protection against cyber criminals and state abuses. How can reconciliation happen between the rebellious and sometime paranoiac attitude against the State and the accountability they put back on the Government's leadership in that context? What failed is the question and how can we foster public debates and education by drawing ethic's parallel between the physical and the cyber world will be at the core of this presentation.