**DS-7-2015: Value-sensitive technological innovation in Cybersecurity**

**CANVAS**
**Constructing an Alliance for Value-driven Cybersecurity**

Start of the Project: September 1, 2016
Duration: 36 Month

**Report for Deliverable D5-4**

# Workshop "Cybersecurity in Business"

| | |
|---|---|
| Deliverable Number | D5-4 |
| Deliverable Name | Workshop 2 Social Sphere "Business" |
| WP Number | WP5 |
| Lead Beneficiary | FSC |
| Dissemination Level | PUBLIC |
| Internal Reviewer | UZH |
| Due date month | Month 18 (February 2018) |
| Date of last Submission («living document») | 16.07.2018 |

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement No 700540 and from the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1.

## Preliminary remark

The reporting of the workshop deliverables is turned into a “living” document, because we were able to organize more than one workshop per social sphere. The report is updated after each completion of a workshop.

According to the current planning, two workshops related to the Sphere “Business” will take place in the context of CANVAS. The current version presents the first workshop that took place on May 28-29 in Helsinki. The second workshop will be combined with the final consortium meeting in 2019 using the contacts of DCU to the ADAPT Centre that includes 140 companies in Ireland and beyond, ranging from indigenous start-ups to multinational enterprises. This second workshop should help disseminate the main output deliverables of CANVAS to the industry.

## Content

# 1. First Workshop: F-Secure, May 28-29, 2018

## 1.1. Outline

The first workshop was organized by FSC in collaboration with BFH and UZH. The workshop took place at F-Secure's premises in Helsinki. The key theme of the workshop was ethics-related challenges that cybersecurity companies and organizations cooperating with those face in their research and operations. Topics discussed in the workshop include:

- Investigation of nation-state cyber operations.
- Vulnerability disclosure and creation of proof-of-concept code for public awareness, incentivizing vulnerability fixing efforts, security research, penetration testing, and other purposes.
- Control of customer devices. Backdoors and use of government sponsored malware as possible countermeasures to ubiquitous use of encryption.
- Ethics, artificial intelligence and cybersecurity.
- Assisting the law enforcement without violating customer privacy, a CERT viewpoint.
- Targeted attacks and ethical choices arising due to attacker and defender operations.
- Privacy and its assurance through data economy and encryption, balancing values with financial interests of companies.

Opinions and observations of cybersecurity practitioners were complemented by representatives of such organizations as ENISA (The European Union Agency for Network and Information Security), ECSO (The European Cyber Security Organisation), CERT-FI (Finnish National Computer Emergency Response Team), Europol EC3 (the European Cybercrime Centre), and others.

Since a number of issues discussed in the workshop were quite sensitive, the workshop was held under the Chatham House rule (in particular, no recording policy):

https://www.chathamhouse.org/chatham-house-rule

This should allow the participants to talk more freely. All the quotes from the talks and all the references to the speakers, attendees, and their organizations with respect to the talks and discussions are with the explicit consent of the speakers and attendees.

As a part of the workshop arrangements, Dominik Hermann and Martin Mueller (University of Bamberg) ran and recorded a series of interviews with the invited speakers. The videos will be shown to students who participate in the CANVAS MOOC, forming a core of case studies. Each case study will focus on one or more issues where cyber security and ethical values are in conflict. The participants of the MOOC will later be asked to discuss selected case studies applying the knowledge that they have acquired in previous sessions.

## 1.2. Workshop program

***May 28***

*Alexey Kirichenko, F-Secure*: 10 – 10.10 am.
Introductory words

*Mikko Hyppönen, F-Secure*: 10.10 – 10.55 am.
A keynote

*Alberto Blanco, Universitat Rovira i Virgili, Tarragona*: 11 – 11.25 am.
Presenting the CANVAS White paper: "Technological Challenges in Cybersecurity"

*Roberto Cascella, European Cyber Security Organization*: 11.30 am. – 12.10 pm.
A look into future cyber security directions for social good

Lunch

*Costin Raiu, Kaspersky Lab*: 1 – 1.40 pm.
The perils and pitfalls of researching nation-state cyberspying

*Antti Tikkanen, Google*: 1.45 – 2.25 pm.
Targeted attacks and ethical questions

Coffee break

*Perttu Halonen, NCSC-FI / CERT-FI*: 2.45 – 3.25 pm.
Preserving the privacy of customers and communicating about incidents: how we do it in the NCSC-FI

*David Wright, Trilateral Research*: 3.30 – 4.15 pm.
At the nexus of ethics, AI and cybersecurity

*Jeroen van der Ham, the National Cyber Security Centre in the Netherlands*: 4.20 – 5 pm.
Vulnerability disclosure and ethical dilemmas faced when dealing with that topic

***May 29***

*Olaf Pursche, AV-Test*: 9.30 – 10.10 am.
Testing IoT – Missing Security & Privacy

*Rickard Carlsson, Detectify*: 10.15 – 10.55 am.
When is ethical hacking ethical?

Coffee break

*Nicole Samantha van der Meulen, Europol EC3*: 11.15 – 11.55 am.
Cybersecurity solutions and challenges faced by law enforcement

*Demosthenes Ikonomou, ENISA*: 12 – 12.40 pm.
On the use of encryption and backdoors - An EU perspective

Lunch

*Florian Grunow, ERNW*: 1.30 – 2.10 pm.
Ethical challenges of security assessment and investigation activities

*Sean Sullivan, F-Secure*: 2.15 - 2.55 pm.
Notes on the threat landscape and F-Secure's operations

Markus Christen, other CANVAS partners
Closing words 3 – 3.30 pm.

### 1.3. Speakers and attendees

**Rickard Carlsson** is CEO of Detectify, a Stockholm-based security startup that provides website security services for developers. He was selected as one of the Sweden's Super talents 2015 by the Swedish business publication Veckans Affärer. Rickard lived and worked in Sweden, USA, and India. He holds MSc in applied physics and electrical engineering and has extensive experience from working as a strategy consultant at McKinsey & Co.

**Roberto Cascella** works as Senior Policy Manager at the European Cyber Security Organisation (ECSO) supporting the activities of WG1 on standardization, certification, labelling and supply chain management, as well as, WG6 on the Strategic Research and Innovation Agenda. He previously worked as Innovation and Research Project Manager (Trust-It Services 2015-16), contributing to H2020 projects on cyber-risk management, privacy and security, cloud computing, and big data. Prior to that, he was a research scientist at University of Trento (2003-08) working on trust and reputation management systems and at INRIA in Sophia Antipolis (2009-10) as Post-doc on statistical approaches for Internet traffic classification, and in Rennes as technical manager (2011-14) of the FP7 Contrail project and the EIT ICT Labs VEP-S activity on cloud computing. He holds a PhD (2007) in ICT from the University of Trento and MSc in Telecommunication Engineering from Politecnico di Torino and from KTH Stockholm in 2003.

**Florian Grunow** is security analyst at ERNW. He holds a Master of Science degree in Computer Science with a focus on software engineering. His research focus is on the security of medical devices. He leads the team responsible for performing security assessments at ERNW and is CEO of ERNW Research.

**Perttu Halonen** joined the National Cyber Security Centre Finland (NCSC-FI) in 2014. His tasks include incident response coordination in CERT function and cooperation network coordination and facilitation on healthcare sector and generally regarding the use of IoT. He holds Master of Science (technology) degree from Helsinki University of Technology. Prior to NCSC-FI, he worked as a research specialist at Nokia. His free time, as much as his family allows, he spends in volunteer fire brigade.

**Jeroen van der Ham** is assistant professor of Computer Network Security in the Design and Analysis of Communication Systems (DACS) group at the University of Twente. Jeroen combines this with his work at the National Cyber Security Centre in The Netherlands (NCSC-NL). At NCSC-NL, he focuses on many developments in coordinated vulnerability disclosure and ethics of the security profession. At the University of Twente he focuses on ethics of Internet security research, denial of service attacks, and anonimization in network measurements.

**Mikko Hyppönen** is Chief Research Officer of F-Secure Corporation. He has written on his research topics for the New York Times, Wired and Scientific American and lectured at the Universities of Oxford, Stanford and Cambridge. He sits in the advisory boards of EUROPOL and the Monetary Authority of Singapore.

**Demosthenes Ikonomou** joined the European Network and Information Security Agency (ENISA) in 2008 and currently holds the position of the Head of Operational Security Unit. He received his MSc in Electronics and Computer Sciences and his PhD in applied sciences from the University of Southampton, United Kingdom, in 1992 and the Université catholiquue de Louvain-la-Neuve (UCL), Belgium, in 2002 respectively. Between 1996 and 2008, he worked for DG Information Society & Media (INFSO)

of the European Commission (now DG CONNECT) mainly involved in the management of R&D projects in the fields of wireless and personal communications as well as networked media.

**Alberto Blanco Justicia** is a postdoctoral researcher at Universitat Rovira i Virgili. He obtained an MSc in Computer Security in 2013 from Universitat Rovira i Virgili, and his PhD in Computer Engineering and Mathematics of Security from the same university in 2017, with a thesis focused on the reconciliation of privacy, security and functionality in e-commerce applications. His research interests are data privacy, data security and cryptographic protocols. He has been involved in several European and national Spanish research projects, as well as technology transfer contracts with Google and Abertis Telecom.

**Nicole S. van der Meulen** has been working in the field of cybersecurity for over a decade. She is currently Senior Strategic Analyst at the European Cybercrime Centre (EC3) at Europol. In that capacity, she functions as Team Leader of the Strategy & Development team. Prior to her arrival at EC3, she was an Advisor of Security Affairs at the Dutch Banking Association. Previously, she led the cybersecurity part of the Defence & Security team at RAND Europe in Cambridge, UK, where she worked as an analyst and led studies for a number of clients, including the European Parliament, the European Union Agency for Network and Information Security (ENISA) and the Dutch Ministry of Security & Justice. Between 2010 and 2012, she worked as a Cyber Security advisor at GOVCERT.NL, the predecessor to the Dutch National Cyber Security Centre (NCSC-NL), where she was co-responsible for the development of the first Cyber Security Threat Assessment, before returning to academia at the start of 2012 as an Assistant Professor at the Department of Transnational Legal Studies at the VU University in Amsterdam. In 2010 she obtained her PhD based on a comparative study between the United States and the Netherlands on digital financial identity theft at the Law Faculty of Tilburg University. She studied Political Science with a focus on International Relations and Comparative Politics at the University of Maryland, Baltimore County (Bachelor of Arts, 2005, Cum Laude) and VU University Amsterdam (Master of Science, 2006, Cum Laude).

**Olaf Pursche** is CCO of the AV-TEST Institute in Magdeburg, Germany. As a student of law and economics in the early 1990s, he worked at the Institute of Law and Informatics of the Leibniz University of Hannover. He joined PC Professionell Magazine, wrote on the topics of Computer & Law and tested security software and Internet services for several years. He developed the IT security editorial and testing division of Europe's largest computer magazine, COMPUTER BILD, which he headed for 15 years, and wrote for several newspapers like BILD and Welt. Since 2015, he is responsible for communications and press relations and heads the marketing department of the AV-TEST Institute. He is a member of advisory boards of public authorities and trade associations.

**Costin G. Raiu is** Director, Global Research and Analysis Team (GReAT), Kaspersky Lab, Romania. Costin specializes in analyzing advanced persistent threats and high-level malware attacks. He joined Kaspersky Lab in 2000 and now leads GReAT at Kaspersky that researched the inner workings of Stuxnet, Duqu, Carbanak and more recently, Lazarus, BlueNoroff, Moonlight Maze and the Equation group. Costin's work includes analyzing malicious websites, exploits and online banking malware. Costin has over 24 years of experience in anti-virus technologies and security research. He is a member of the Virus Bulletin Technical Advisory Board, a member of the Computer AntiVirus Researchers' Organization (CARO) and a reporter for the Wildlist Organization International. Before joining Kaspersky Lab, Costin worked for GeCad as Chief Researcher and as a Data Security Expert with the RAV antivirus developers group.

**Sean Sullivan** is Security Advisor and researcher at F-Secure. He joined F-Secure (Security Labs) in 2006. Based in Helsinki, he works with a dynamic group of cyber security experts from over dozen countries. He works primarily with the analyst teams that handle the classification of incoming malware samples

and develop antimalware automation, and secondarily with the research teams that develop new antimalware technologies. Sean is an active member of “InfoSec Twitter” and participates in academic events. He has briefed government officials and technical experts from around the world on computer security issues and antimalware technologies. In addition, he is frequently interviewed by media worldwide. Prior to F-Secure, Sean worked in the desktop/application support field for over ten years and has a great deal of experience working with malware victims "in-the-field".

**Antti Tikkanen** works with the Threat Analysis Group at Google as Engineering Manager. His team protects both Google and its users against nation-state sponsored attackers. Previously, Antti worked with F-Secure Corporation for 10 years in various roles related to malware analysis, research and software engineering. He holds the Master of Science degree in Computer Science from the Aalto University, Finland.

**David Wright** is Director of Trilateral Research Ltd, a London-based company he founded in 2004. He has published more than 60 articles in peer-reviewed journals, and co-edited and co-authored several books, including *Privacy Impact Assessment* (Springer, 2012) and *Surveillance in Europe* (Routledge, 2015). He coined the term and published the first article on ethical impact assessment.

Contribution of the following CANVAS partners and representatives of several organizations in Finland, who attended the workshop, shared their views, and raised questions, was highly appreciated:

- Bengt Sahlin, Ericsson
- David-Olivier Jaquet-Chiffelle, University of Lausanne
- Dominik Hermann, University of Bamberg
- Emad Yaghmaei, TU Delft
- Endre Bangerter, Bern University of Applied Sciences
- Fritz Alder, Aalto University
- Gwenyth Morgan, Dublin City University
- Ilona Usvapelto, the University of Helsinki
- Janika Tyynelä, VTT
- Josep Domingo-Ferrer, Universitat Rovira i Virgili, Tarragona
- Juha Roning, Oulu University
- Karmina Aquino, F-Secure
- Lina Jasmontaite, VUB
- Markus Christen, University of Zurich
- Martin Mueller, University of Bamberg
- Matti Aksela, F-Secure
- Mikko Karikytö, Ericsson
- Päivi Tynninen, F-Secure
- Salome Stevens, University of Zurich
- Tuomas Aura, Aalto University
- Veikko Ikonen, VTT

### 1.4. Summaries of the talks

In the keynote, **Mikko Hyppönen** talked about the evolution of cyberattacks from semi-innocent experiments, through hooliganism, to financially motivated organized crime and state-sponsored opera-

tions. Specific ethical challenges of cybersecurity companies related to the use of malware by governments and law enforcement agencies (and mistakes and dangers it brings) and to hiring people skilled but previously involved in cyberattacks and similar illegal activities were discussed.

**Alberto Blanco** presented the CANVAS White paper "Technological Challenges in Cybersecurity": https://ssrn.com/abstract=3091942 to introduce the CANVAS work to the attendees. The focus was on the values of privacy, autonomy and fairness.

**Roberto Cascella** gave a quick overview of the current state of play of cybersecurity in Europe, moving then to a vision for the development of the European cybersecurity ecosystem towards 2027. He then presented the research priorities identified in the ECSO Strategic Research and Innovation Agenda, viewing cybersecurity as an essential enabling factor for the development and exploitation of digital technologies and innovation. During the talk, Roberto also discussed his personal views on the implications of technology for the society and citizens, using IoT technology as a practical example and indicating what could be done to prepare to innovations towards social good. In the discussion, it emerged that ethical hacking could be beneficial both in terms of strengthening the security of products, services and systems, with impact on their evaluation and certification, and in terms of improving the cyber security skills towards a proactive cyber security. A number of growing concerns were considered, including: "digital divide" of citizens in terms of their expertise; constant monitoring to ensure security vs. misuse of data; the need for automated reasoning vs. potential data pollution and uncertainty about how decisions are made.

In his talk, **Costin Raiu** presented the history of and current activities in Advanced Persistent Threat (APT) research at his company and associated risks. In particular, such questions as:

- Criteria for selecting what to research in depth
- What to publish and what not?
- When is the right time to publish something?

were discussed, illustrated via real-life examples. Many difficult choices for cybersecurity industry related to unclear intentions of attackers, lack of trust in governments, conflicting interests of various groups and states, etc. were considered. Costin also talked about more recent issues brought by such phenomena as supply chain attacks, mobile malware, social media manipulation, and "hacking as a service".

**Antti Tikkanen**'s talk focused on ethical challenges arising in the work of people researching and defending against APT attacks. From discovering, researching, and engaging with attackers, Antti reviewed scenarios where defenders face a challenge of finding a path, which both is ethical and meets their operational needs. Examples, illustrated by real-life cases, included the use of telemetry while preserving customer privacy, attributing and publishing information about campaigns, probing attacker infrastructure, hacking back. One serious complication is that the same malware can be used for very different intentions and by very different groups, which is why "selective detection" is a very dangerous choice for cybersecurity companies. In addition, challenges of attribution, becoming highly important with the growth of targeted attacks, were discussed.

Challenges of CERT operations and policies and practices for addressing those were presented by **Perttu Halonen**. If customers fear that a CERT might disseminate information about their security incidents in a way that would lead to bad publicity or cause repercussions, they are less likely to give useful information to the CERT. On the other hand, CERTs are supposed to disseminate to the constituency and to other stakeholders some information about security incidents they have handled. Information sharing with colleagues is the best weapon for CERTs to fight malicious hacking, and the police and security intelligence service are essential partners for NCSC-FI. The police, in turn, is obliged to

investigate any crime they are informed of. However, the choice to report an offense should be with the crime victim, not with the CERT. Perttu's talk reviewed principles and procedures for CERTs to protect privacy of their customers while communicating to third parties about incidents, such as openness about information sharing, proper information classification, agreements upon acceptable use of shared information, and use of the Chatham House rule.

In his talk, **David Wright** discussed examples of ethical issues connected to potential use of AI in cyberattacks and its role in the arms race between attackers and defenders, including challenges related to counterattacks. Also in the focus were various ways of dealing with AI dangers, in particular, regulatory measures, including such questions as: Should AI research be controlled? How can such control be implemented? Could self-regulation and codes of practice be effective?
An important and controversial issue of counterattacks and utilization of AI in those was considered, focusing on challenges related to:

- Potential collateral damages brought by counterattacks
- Uncertainties with respect to true culprits and accusations without evidence
- Proportionality of countermeasures
- Tradeoffs between transparency and guarding sensitive information about discovered attacks

With all the subtleties presented, the conclusion was in favor of counterattacking, since not doing that will encourage attackers to carry on with their operations.

**Jeroen van der Ham** talked about vulnerability disclosure and ethical dilemmas involved. Some of the key challenges discussed range from dealing with vulnerability reporters who cross the line, for example, in going short on a company that they found vulnerabilities in, to vulnerabilities that were most likely discovered by intelligence services years before it became public, after which it created a worldwide crisis. Several cases were presented to illustrate Public Prosecutor Service judgements on what is justified and what is disproportionate in vulnerability disclosure activities and to show attitude of organizations responsible for found vulnerabilities. Jeroen also discussed certain findings in an interesting NTIA report on Vulnerability Disclosure Attitudes and Actions, in particular, expectations and motivation of vulnerability researchers.

Issues related to low or non-existing security of many popular IoT devices were discussed by **Olaf Pursche**. In particular, many companies have to deal with trade-offs between investments into product security and customer privacy protection and business targets. The attention in the talk was paid to such questions as: Does every product necessarily have to be connected to the Internet? What does a product have to guarantee when connected to the Internet? What risks can be posed by products that neglected security and privacy in product development? Based on practical examples from several years of the AV-Test device testing practice, the presentation demonstrated the lack of IT security and privacy in widely used IoT products. The dangers resulting from this were mentioned and solutions suggested.

**Rickard Carlsson**'s talk focused on the ethical dilemmas that pervade white-hat hacking, bug bounty and responsible disclosure programs, and – more generally – organization of the vulnerability market, including market values of discovered bugs. He presented well-known incidents of grey zone hacking, such as the "Instagram's Million Dollar Bug" that grew into a public discussion on the ethics of bug bounty between a security researcher and Facebook's CISO Alex Stamos. Another example was Google Project Zero: Is the initiative ethical even though disclosures of unpatched vulnerabilities allow anyone to access information that could be used for malicious purposes? Rickard also shared certain challenges of and insights into the collaboration Detectify had with the white-hat hacker community through their security platform Detectify Crowdsource. Today, Crowdsource has over 100 members and provides valuable security research that helps protect Detectify's customers, contributing over 250

unique vulnerabilities to Detectify vulnerability scanner. More than one third of these submissions are 0-days, which means Detectify had to create their own Vulnerability Disclosure Guidelines.

The talk by **Nicole Samantha van der Meulen** discussed challenges for law enforcement introduced by the enhanced use of encryption, along with other developments, in particular with regard to access to data. Whilst these developments can have a beneficial impact on cyber security, they can also be abused by criminals, which creates a difficult situation where solutions require creativity and may involve tradeoffs. Looking ahead, there are more challenges on the horizon for law enforcement with respect to new technological developments. The question then becomes how we can include the needs of the law enforcement community. And if these needs are not included, what sort of consequences may we potentially face as a society? The talk aimed to illuminate the challenges faced by law enforcement to contribute to a comprehensive picture of new developments in the realm of digital technology to ensure that any way forward would engage in conscious risk taking, based on as much information as possible. Dangers of arguments based on inaccurate statistics or incomplete information were also considered.

**Demosthenes Ikonomou** talked about ethics in intelligence, encryption and backdoors, and vulnerability disclosure. In particular, in the debate on the use of backdoors, the view of ENISA is negative, since that will lead to higher risks for the citizens, while criminals will likely find other strategies ("Technology beats regulation"). Several problems related to vulnerability disclosure were mentioned, including legal challenges, lack of vendor and researcher maturity, and vulnerability acquisition for national intelligence. ENISA strongly advocates a higher attention to be paid to ethics in teaching cyber intelligence and communicating on cybersecurity matters.

**Florian Grunow** discussed ethical challenges in security assessment and investigation activities, focusing on ethical considerations related to disclosures and accidental findings, digital forensics and incident response operations, and investigation of social engineering cases. Examples of difficult questions are:

- Dealing with customers that want security assessment to bring a specific result or care only about receiving a compliance report.
- Dealing with customers that want to conceal found problems.
- Security consultant behavior in cases where investigations found something illegal or unethical that the customers do.
- Ethics of penetration testing, in particular, involving social engineering activities (e.g., security consultants have to lie to people).
- Security consultants' feelings towards their customers and how those feelings influence their activities: business vs. research interests vs. ethical considerations.

Florian also talked about the internal ethics committee at his company.

In the last workshop talk, **Sean Sullivan** shared historical notes on the threats and F-Secure's activities in protecting their customers and went on to discuss current challenges related to modern technology, law, citizens' perception of threats, psychology and goals of criminals, and transparency of technology and service providers.

### 1.5. Final notes

We conclude with two questions raised in the talks that generated especially intense and interesting discussions during and after the workshop. The first was about situations when cybersecurity vendors receive requests of ignoring certain activities and attack tools. The "slippery slope" wording, used by

one of the speakers in connection with considering such requests, was repeated many times in the talks and discussions. The other question, mentioned by a number of attendees as deserving special attention, was about sharing results of cybersecurity research and investigations, which can be considered a hard instance of the general issue of researchers' moral responsibility and dangerous knowledge.