Cybersecurity and Ethics

Bart Preneel
COSIC KU Leuven
Firstname.lastname@esat.kuleuven.be
@bpreneel1
preneel@infosec.exchange
SecAppDev
2 June 2026

KU LEUVEN COSIC

1

Outline

- What is ethics?
- Cybersecurity trends with ethical impact
- Summary
- Cases

2

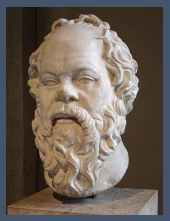
2

What is ethics? (moral philosophy)

The discipline concerned with what is morally good and bad and morally right and wrong. The term is also applied to any system or theory of moral values or principles.

Britannica

Babylonian Code of Hamurabi, Legal text from ca 1750 BC



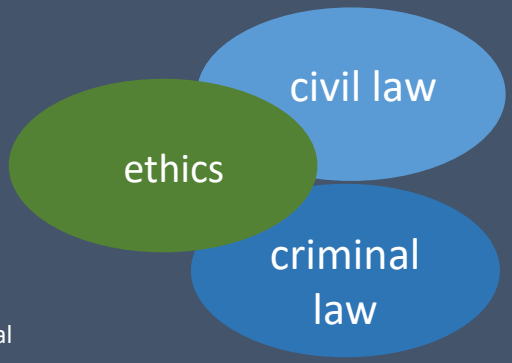
Socrates, 470-399 BC

"love of wisdom" (φιλοσοφία), not experience, is the way to acquire the competency involved in living the good life

3

3

Ethics should not be confused with law



Any act can be independently (il)legal or (un)ethical

4

4

Ethics for scientists and engineers

Bombing of Hiroshima, 1945

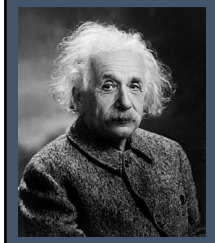
Dr. Karl Brandt, Nuremberg Trial 1946-1947

Children spraying DDT, 1953

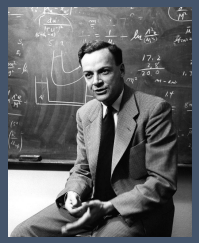
5 Slide credit: Phil Rogaway

5

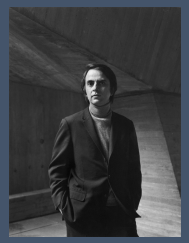
Role models: ethics of responsibility



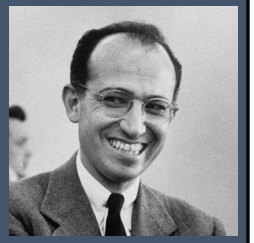
Albert Einstein



Richard Feynman



Carl Sagan



Jonas Salk

Russell-Einstein manifesto, 1955

6 Slide credit: Phil Rogaway

6

Approaches to ethics

Virtue ethics: VALUES	Deontology STANDARDS	Utilitarianism: OUTCOMES
• Character • Intentions • Motives • Attitude	• Duty • Rules • Means • Consistency	• Consequences • Goals • Ends • Results

7

7

Approaches to ethics: values

Virtue ethics: VALUES

- Character
- Intentions
- Motives
- Attitude

8

8

Approaches to ethics: standards as professional, do harm, no good

Deontology STANDARDS

- Duty
- Rules
- Means
- Consistency

THE UK CYBER SECURITY COUNCIL CODE OF ETHICS

The UK Cyber Security Council's Code of Ethics for participating organisations (Member Organisations) is at the heart of the Council's operations and terms of reference.

The Code of Ethics is a set of values and principles, which influence judgement and guide Member Organisations to conduct business honestly and with integrity. It details ethical standards and provides guidance on behaviour and decision-making in difficult situations, particularly where there are conflicting pressures or considerations which need to be reconciled.

The Code may be summarised as follows:

- demonstrate integrity, professionalism and responsibility, and respect for others
- uphold the reputation of the cyber security sector
- repudiate any and all acts of bribery, corruption and extortion
- uphold laws, regulations, standards and technical rules

9

9

Deontology

- People have fundamental rights, e.g.
  - privacy
  - self-agency
  - informed consent
- Moral actors have a duty to respect those rights
- Kant's "Categorical Imperative"
  - one should not violate any single person's rights in order to accomplish another objective
  - human beings should be treated as "ends and never purely as means"

10

10

ACM Code of Ethics

https://www.acm.org/code-of-ethics

1. GENERAL ETHICAL PRINCIPLES

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing

1.2 Avoid harm

1.3 Be honest and trustworthy

1.4 Be fair and take action not to discriminate

1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts

1.6 Respect privacy

1.7 Honor confidentiality

11

IEEE Code of Ethics

https://www.ieee.org/about/corporate/governance/

I. To uphold the highest standards of integrity, responsible behavior, and ethical conduct in professional activities.

1. to hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and sustainable development practices, to protect the privacy of others, and to disclose promptly factors that might endanger the public or the environment;
2. to improve the understanding by individuals and society of the capabilities and societal implications of conventional and emerging technologies, including intelligent systems;
3. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
4. to avoid unlawful conduct in professional activities, and to reject bribery in all its forms;
5. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, to be honest and realistic in stating claims or estimates based on available data, and to credit properly the contributions of others;
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;

II. To treat all persons fairly and with respect, to not engage in harassment or discrimination, and to avoid injuring others.

7. to treat all persons fairly and with respect, and to not engage in discrimination based on characteristics such as race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression;
8. to not engage in harassment of any kind, including sexual harassment or bullying behavior;
9. to avoid injuring others, their property, reputation, or employment by false or malicious actions, rumors or any other verbal or physical abuses;

III. To strive to ensure this code is upheld by colleagues and co-workers.

10. to support colleagues and co-workers in following this code of ethics, to strive to ensure the code is upheld, and to not retaliate against individuals reporting a violation.

12

IEEE CYBER SECURITY

https://cybersecurity.ieee.org/policyethics/
until October 2025

HOME | INTERVIEWS | DESIGN | TRY | READ | ATTEND | INVITE | ABOUT

RECENTLY PUBLISHED | OCTOBER 1, 2018 | SAVE THE DATE FOR SECDEV 2019

HOME | POLICY/ETHICS

Policy/Ethics

Cybersecurity impacts both public policy and ethics. We will have more information soon.

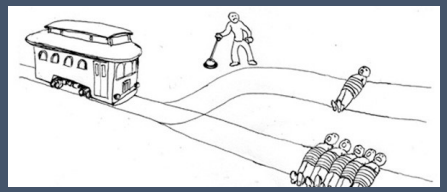
13

Approaches to ethics: utilitarianism

Utilitarianism: OUTCOMES

- Consequences
- Goals
- Ends
- Results

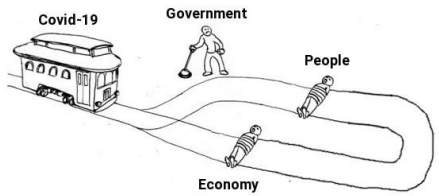
Example: the trolley problem

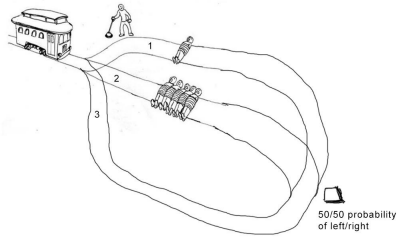


14

14

The trolley problem





15

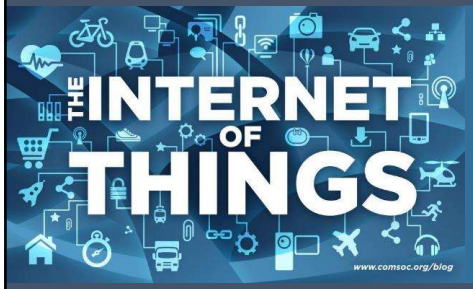
Outline

- What is ethics?
- Cybersecurity trends with ethical impact
- Summary
- Cases

16

16

IoT makes IT more intrusive

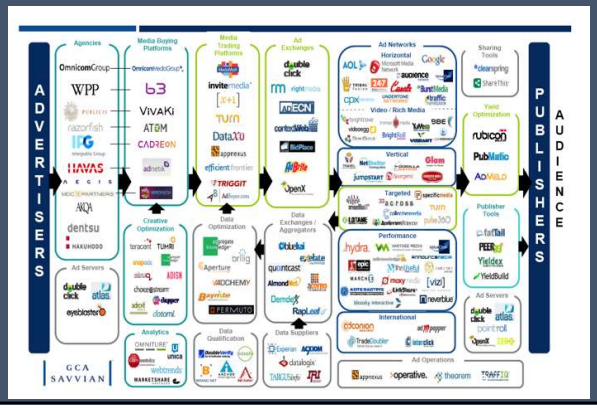


Intrusive
unavOidable
sTealthy

17

17

Andrew Lewis: If you are not paying for it, you're not the customer; you're the product being sold



19

"The cloud is someone else's computer"

Safe Harbor (2015)

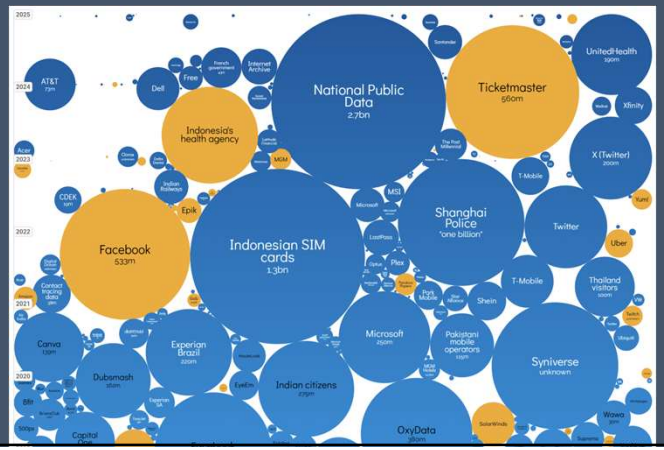
Privacy Shield (2020)

EU-U.S. Data Privacy Framework (2026?)

18

World's biggest data breaches

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks



20

A metaphor

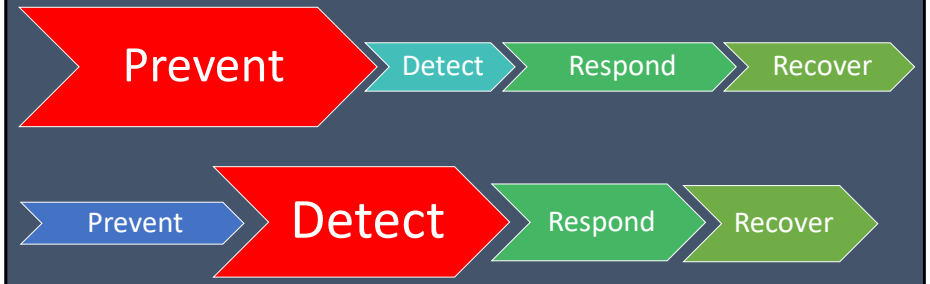
Thinking of
Big Data in terms of pollution

21

Big Data and Data Analytics (AI) for Security

22

Paradigm shift (2000s)



23

Big Data for security

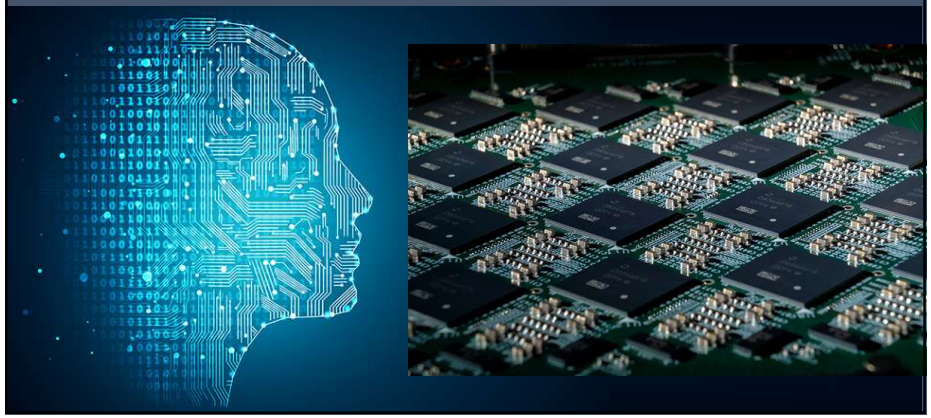
If you have no visibility of your systems, how can you secure them?

Prevention is hopeless: if you detect all incidents, you can stop the bad guys in a cost-effective way (read: you can reduce investments in prevention)

By applying analytics (AI) to incident data sets, we can learn how the bad guys behave and detect them even faster next time around

24

AI: ability of a machine to display human-like capabilities such as reasoning, learning, planning and creativity



25

Biometrics: facial recognition

Clearview AI's Database Has Amassed 10 Billion Photos

> 1 billion smartphone with face recognition features

26

1 billion surveillance cameras '21

54% of these in China

Ningbo 2019

27

Law Enforcement Uses AI

BELGIAN POLICE USED CLEARVIEW AI MUCH MORE THAN THOUGHT – IT PRO – NEWS

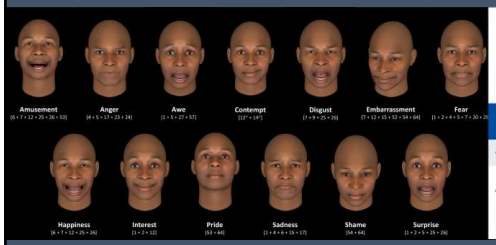
March 10, 2022 World 0 Views

Not 2x but 78 times
No valuable results

500+K cameras in Belgium of which 4500 "smart" (ANPR)

28

Next Step: Emotion Recognition



29

The AI Panopticon:
Continuous monitoring and analysis of all humans and devices

30

AI and Cybersecurity

Credit: Vera Rimmer

31

AI Helping Cybersecurity

Unthinkable without AI

- Malware detection
- Intrusion detection
- Vulnerability detection
- Fraud detection: transactions, domain registrations
- Phishing detection
- Data loss prevention
- Side channel analysis

Questions to ask

- How reliable? (false positives/negatives)
- Adaptive adversaries?

32

The Dark Side of AI

- Spear phishing attacks
- Automation of cyberattacks: all MITRE stages resulting in lower barrier of entry
- Misinformation and deepfakes
- Hallucinations
- Data feedback loops
- Unpredictabiltiy

Clark Barrett et al. Identifying and Mitigating the Security Risks of Generative AI, 2023, https://arxiv.org/abs/2308.14840

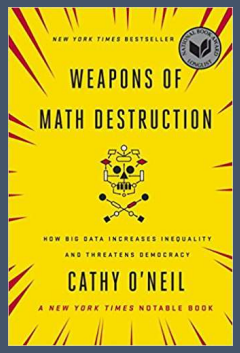
33

AI War: Machine versus Machine

Joysula Rao, USING AI FOR SECURITY AND SECURING AI in Robust Machine Learning Algorithms and Systems for Detection and Mitigation of Adversarial Attacks and Anomalies: Proceedings of a Workshop (2019)

34

Algorithmic fairness and bias



https://towardsdatascience.com/a-gentle-introduction-to-the-discussion-on-algorithmic-fairness-740bbb469b6

35

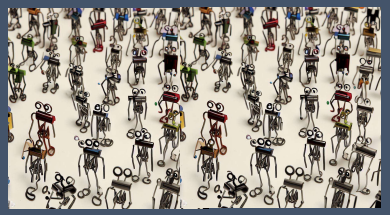
36

The AI Debate

Credit: Scot Aaronson/Boaz Barak: Five worlds of AI https://scottaaronson.blog/?p=7266

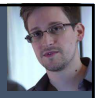
AI Ethics
Worried about AI-Dystopia

AI Alignment
Worried about "Paperclipalypse"



37

SSO: Special Source Operations



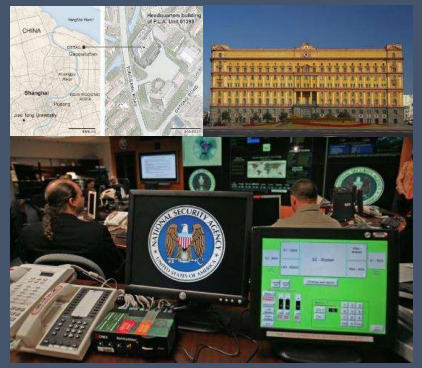
1. PRISM (server)

2. Upstream (fiber)

XKeystore or Tempora

39

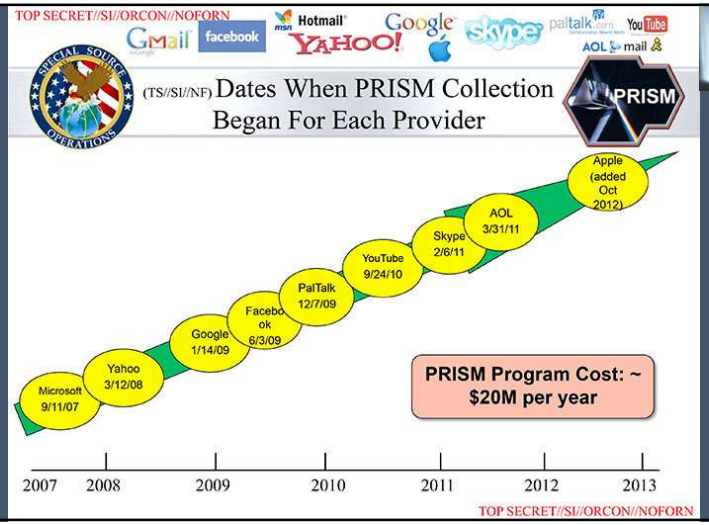
Law enforcement and nation state hacking resulting in cyber arms proliferation

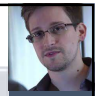


38

38

PRISM



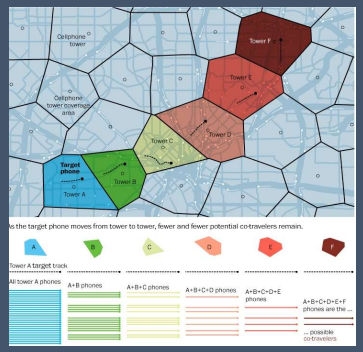


40

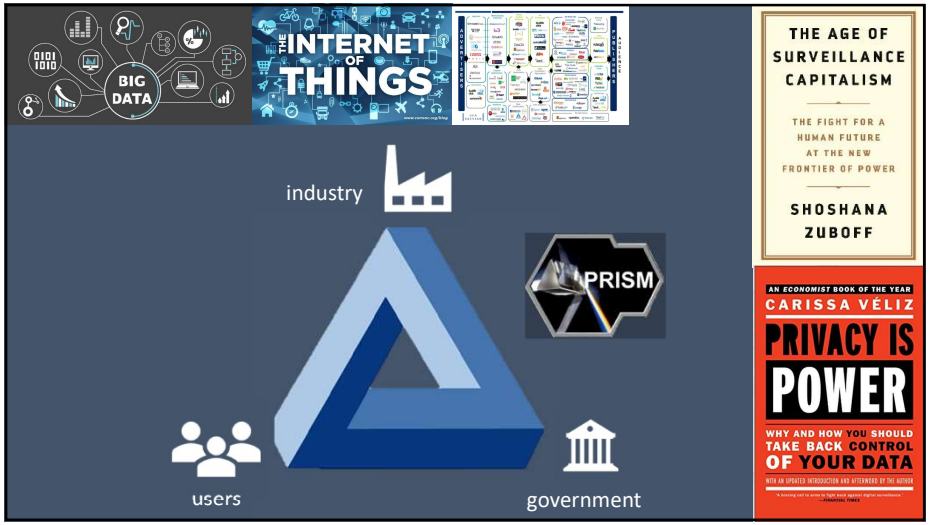
SSO: Special Source Operations

3. Metadata

(2013)
NSA collects about 5B records a day on cell phone location
Co-traveler



41

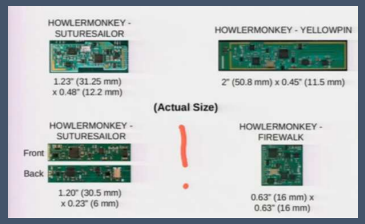


43

TAO: Tailored Access Operations

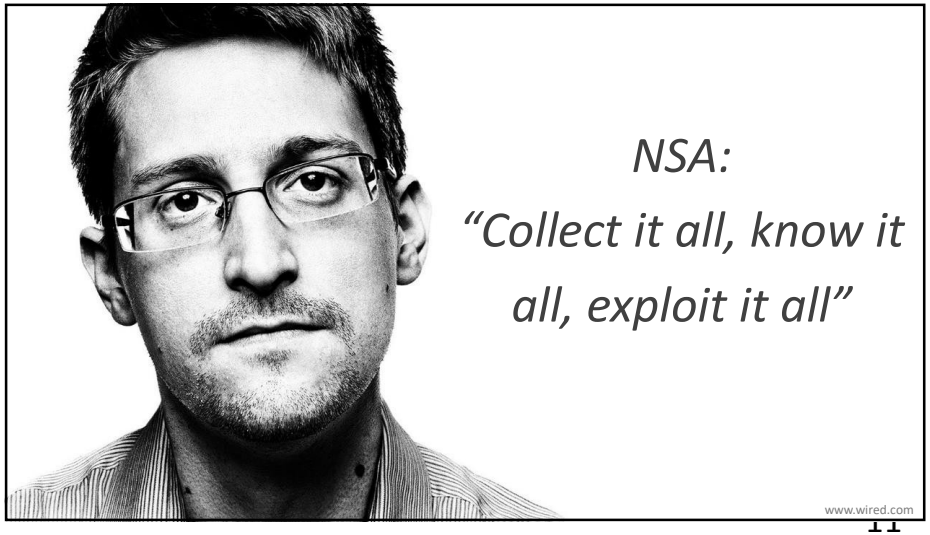
Many technologies

large number on bridging air gaps
number of targets is limited by cost/effort



Examples:
- use radio interfaces and radar activation
- supply chain interception
- FOXACID: A system for installing spyware with a "quantum insert" that infects spyware at the packet level

42



44

Beyond law enforcement: rogue companies and 0-days

45

(Part of) government seems to prefer offense over defense

How many 0-days do the NSA, FBI, and CIA have?

Are they revealed to vendors?

If so when?

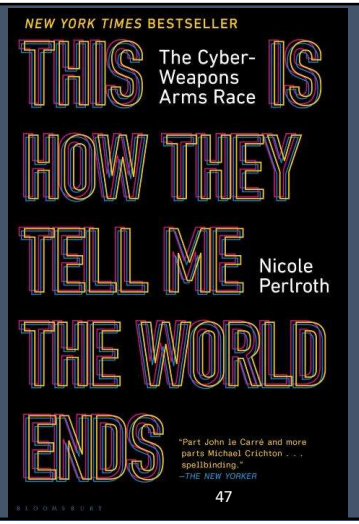
0-days stolen by Shadow brokers from Equation Group resulting in Wannacry, Petya, not-Petya

US$ 250 M loss for Maersk

46

46

The market for 0-days



47

47

Vulnerability Disclosure

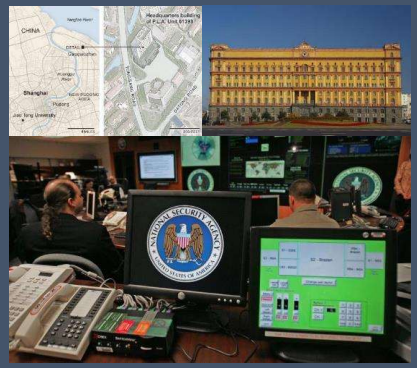
- Coordinated Vulnerability Disclosure https://en.wikipedia.org/wiki/Coordinated_vulnerability_disclosure
  - Disclose vulnerability to vendor
  - Only release to public after delay (3-12 months)
- Bug bounty programs/platforms https://en.wikipedia.org/wiki/Bug_bounty_program
  - Financial compensation for finding and disclosing vulnerability
  - E.g. EU-FOSSA 2

48

48

Sed quis ipse custodiet custodes?

But who shall watch over the guards?



49

Outline

- What is ethics?
- Cybersecurity trends with ethical impact
- Summary
- Cases

50

50

Ethics and technology

- Technologies are not ethically neutral
- Fast evolution
- Technology is magic for a large part of society (including lawmakers)
- Technology reshapes power

51

51

Ethics and cybersecurity

- Harms to privacy: governments, industry, citizens
- Harms to property: Stuxnet, ransomware
- Cybersecurity resource allocation: building insecure systems due to lack of resources and budget
- Transparency and disclosure
- Cybersecurity roles, duties and interests

Complex issues
but answers are not necessarily subjective

52

52

Ethics and cybersecurity: goals

- Goals itself: mass surveillance, malware
  - key escrow, Child Sexual Abuse Material detection, military use
- Impact on personal safety: drones, autonomous vehicles
- Unintended consequences: medical devices
- Abuse by malicious actors
- Military use:
  - defense versus offense
  - drones, robots

53

53

Ethics and cybersecurity: governance

- Involve stakeholders
- Risk mitigation
- Vulnerability disclosure
- Incidental findings

54

54

Chaotic Eclipse" (aka Nightmare-Eclipse) (R) versus Microsoft (M)

- R disclosed 6 alleged Windows zero-day vulnerabilities over several weeks affecting **Windows Defender, BitLocker, and CTFMON** components.
  - 3 vulnerabilities (**BlueHammer, RedSun, and UnDefend**) reportedly actively exploited in the wild
- R: “M ignored vulnerability reports, closed tickets without explanation, and deleted the account used for submissions.”
- M: “vulnerabilities were publicly disclosed without prior coordination, increasing risk to customers”
- Vulnerabilities added to Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities **(KEV)** catalog, triggering federal remediation requirements.
- Shortly after the disclosures, the R's accounts were reportedly removed from both **GitHub** and **GitLab**
- R: further disclosure or announcement planned for July 14

55

55

Ethics and cybersecurity: analysis methods

- Systems
  - Vulnerability disclosure: e.g. RSA keys*
  - Bug bounty programs
- Lab study versus field study
  - Large scale scanning
  - Cyberphysical systems
- Attacks: honeypots, malware, spyware, ransomware, botnets,…

* A.K. Lenstra, J.P. Hughes, M. Augier, J.W. Bos, T. Kleinjung, C. Wachter: Public Keys. CRYPTO 2012: 626-642
* N. Heninger, Z. Durumeric, E. Wustrow, J.A. Halderman: Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices. USENIX Security Symposium 2012: 205-220

56

56

Ethics and cybersecurity: design methods

- Systems
  - Gaydar (2009): research tool exposed sexual orientation of Facebook users by crawling their friendship relations (Jernigan and Mistree, 2009); run on the Facebook accounts of 6,077 students associated with MIT
  - https://pleaserobme.com (2010)
- Attacks
  - Cryptanalysis
  - Cryptanalysis tools Aircrack-ng tool
  - Pen-testing tools
  - Malware design tool
- Human factors
  - Consent versus covert research
  - Vulnerable populations

57

57

Computer security example

source: https://securityethics.cs.washington.edu

- Company A produces a lifesaving wireless implantable medical device. It is the only device of its type on the market. When a patient receives this device, it will (on average) extend their lifespan by 10 years
- Company A goes bankrupt because the condition is rare and not many people use the device. However, there are many devices still available (already produced), many devices are already implanted in patients, and doctors still implant the (now unsupported) device in new patients that need it
- Later, researchers discover a software vulnerability in the device. If exploited, the vulnerability could cause significant harm to the patients. Since Company A no longer exists, the software cannot be updated to address this vulnerability
- The likelihood of security compromise is zero (regardless of whether disclosed or not)
- Question: What should the researchers do? Disclose the vulnerability to the public? Not disclose the vulnerability to anyone? Talk with the FDA?

58

58

Computer security example

source: https://securityethics.cs.washington.edu

- **If not disclose:** Patients have no awareness that their device is vulnerable; patients keep and/or proceed with obtaining device and receive significant health benefits
- **If disclose:** Patients have the choice to not receive or to remove the device; risk of psychological harm if patients know they have a vulnerable device (even if chance of exploitation is zero); risk of health harm if patients do not receive / remove the device

59

59

Optimism is a moral duty
(Immanuel Kant)

60

Architecture is politics [Mitch Kapor'93]

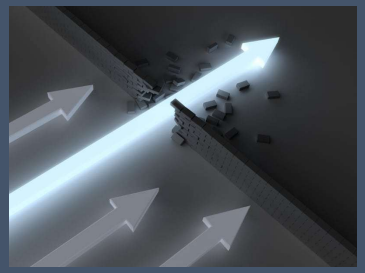
Avoid single point of trust that becomes single point of failure

61

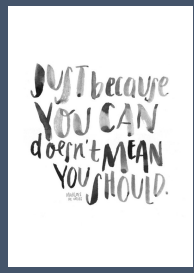
61

Social responsibility

For thousands of years, civilian technology has helped humanity



Technology is not neutral: it reflects values



https://marloesdevries.com/blog/just-because-you-can-doesnt-mean-you-should/

63

Open (source) solutions

Effective governance

Transparency for service providers

EU-FOSSA

EU Free and Open Source Software Auditing

62

62

Bart Preneel

ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven
WEBSITE: homes.esat.kuleuven.be/~preneel/
EMAIL: Bart.Preneel@esat.kuleuven.be
MASTODON: bpreneel@infosec.exchange
TWITTER: @bpreneel1
TELEPHONE: +32 16 321148

KU LEUVEN

ArenBerg Crypto BV

COSIC

64

64

More information (1): Articles

Shannon Vallor, An introduction to Cybersecurity Ethics, https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf

Kevin Macnish, Jeroen van der Ham, Ethics in cybersecurity research and practice, Technology in Society Volume 63, November 2020, 101382, https://doi.org/10.1016/j.techsoc.2020.101382

Tadayoshi Kohno, Yasemin Acar, Wulf Loh: Ethical Frameworks and Computer Security Trolley Problems: Foundations for Conversations. USENIX Security Symposium 2023, https://www.usenix.org/conference/usenixsecurity23/presentation/kohno

Philip Rogaway, The moral character of cryptographic work, Cryptology ePrint Archive, Report 2015/1162

Bart Preneel, Phillip Rogaway, Mark D. Ryan, Peter Y. A. Ryan: Privacy and security in an age of surveillance (Dagstuhl perspectives workshop 14401). Dagstuhl Manifestos, 5(1), pp. 25-37, 2015.

More information (2): Books

The Routledge International Handbook of Engineering Ethics Education, Edited By Shannon Chance, Tom Børsen, Diana Adela Martin, Roland Tormey, Thomas Taro Lennerfors, Gunter Bombaerts, 2025, Routledge, DOI https://doi.org/10.4324/9781003464259, 698 pages (free book)

Glenn Greenwald, No place to hide, Edward Snowden, the NSA, and the U.S. Surveillance State, Metropolitan Books, 2014

Susan Landau, Surveillance or Security? The Risks Posed by New Wiretapping Technologies. MIT Press, 2013

Susan Landau, Listening In: Cybersecurity in an Insecure Age, Yale University Press, 2017

US National Academies, Decrypting the Encryption Debate, 2018, https://www.nap.edu/read/25010/chapter/1

More information (3): Movies and media

Movies

Citizen Four (a movie by Laura Poitras) (2014) https://citizenfourfilm.com/

Edward Snowden - Terminal F (2015) https://www.youtube.com/watch?v=Nd6qN167wKo

John Oliver interviews Edward Snowden https://www.youtube.com/watch?v=XEVlyP4_11M

Snowden (a movie by Oliver Stone) (2016)

Zero Days (a documentary by Alex Gibney) (2016)

Media

https://firstlook.org/theintercept/

http://www.spiegel.de/international/topic/nsa_spying_scandal/

More information (4): Links

Links

https://www.enisa.europa.eu/

https://www.eff.org/nsa-spying/nsadocs

https://cjfe.org/snowden

http://www.europarl.europa.eu/committees/en/libe/subject-files.html?id=20130923CDT71796#menuzone

https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf