C4DT
Center
for Digital
Trust

COURSE PLAN

Foundations of ICT for Lawyers and Policy Workers

DIGITAL TRUST IN INTERNATIONAL AND HUMANITARIAN LAW

Beta course in collaboration with ICRC — March 25–29, 2019

Overview

Monday, March 25

- Think “digital trust”
- Refresher: writing programs
- Refresher: networks and the web
- Refresher: traditional cryptography

Tuesday, March 26

- Cybersecurity

Wednesday, March 27

- Cybersecurity (case study)
- ML and big data

Thursday, March 28

- ML and big data (continued)
- ML and big data (case study)

Friday, March 29

- ML and big data (case study, continued)
- Modern crypto
- Blockchain and smart contracts

Note that this course plan is subject to change, including in the topics covered and the identify of instructors. It is provided for information only. A final course plan will be provided to attendees at the beginning of the course.

Monday, March 25: Reviewing the Fundamentals

09:00 10:30 ☕	Welcome Understanding Digital Trust • What is “digital trust” and how understanding it is becoming essential for data protection lawyers and policy advisers • The stakeholders of a digital trust ecosystem • Understanding the context: threat modelling • A lawyer’s role	Dubochet and Marelli
10:45 12:15 🍽	Refresher: writing programs • How computers are instructed to complete tasks • Connecting modules to make software systems • How vulnerabilities arise in software (and how hard is it to prevent?) • Debugging and testing • A programmers’ work in practice (and how to tell if she’s good) • Software best practices and standards • Security by design • Open source and verifiability	Dubochet
13:15 15:15 ☕	Refresher: networking and web technologies • From hardware to software: network layers • How to scale from computer-to-computer connections to the global Internet? • Vulnerabilities in networks and the Internet • Focus on DNS and its vulnerabilities • The Web: pages as software • Vulnerabilities on web pages • Who controls the Internet?	Monod
15:30 17:00	Refresher: cryptography basics • What does cryptography do: confidentiality, data integrity, authentication, non-repudiation • Encryption in transit, at rest, and in process • Typology of encryption techniques and of their vulnerabilities • Why is “real” cryptography always weaker than in theory? • How much cryptography on the (public) Internet, and how secure is it? • Who controls cryptography?	Monod

Tuesday, March 26: Cybersecurity

09:00 10:30 ☕ 10:45 11:15	Cybersecurity: the big picture • The “attack surface” of an organization • Who are hackers, and what are their motivations? • Understand the cyber kill chain: methodology of an attack • Threat modelling: evaluate cybersecurity relative to threat • The life-cycle of a vulnerability: zero-day, patching cycle, etc. • That *other* vulnerability: phishing and social engineering • What happens on a compromised computer: new vulnerabilities, data collection, use as attack vector, etc. • Selecting software and services for security (best practices for evaluation, certification, sourcing) • The role of security providers (MSSP)	Bost
11:15 12:45 🍕	Network security • The Internet as your computer: Saas, Paas, clouds, etc. • Where is data located, and how to know in practice? • The network as a battlespace: vulnerability scanning, packet inspection, intrusion detection, etc. • A secure space in your network: firewalls, air gaps and other “barriers” • Making a private place on the Internet with cryptography: https, VPNs, cloud encryption	Bost
13:45 14:45 ☕	Attributing cyberattacks • What is attribution and why does it matter? • How does attribution take place, and how well does it work? • Computer forensics basics • Trustworthiness of attribution: understand the principles and the actors • “false flag” operations	Bost
15:00 17:00	Cyberwarfare operations • State-sponsored cyberwarfare: who’s who? • The tools of cyberwarfare • Cyberwarfare case studies: from Iran’s uranium centrifuges to the Ukrainian power grid • The geopolitics of the Internet	Rickli

Wednesday, March 27

Cybersecurity (continued)

09:00 10:30 ☕ 10:45 12:45 🍽	Case study in groups: cyberattack/defense scenario • Role play between “defenders” and “hackers” • Expert assess groups’ choices and discusses potential outcomes	ICON

Machine Learning and Big Data

13:45 14:45	Big Data • Back to basics: what is data and where does it come from? • Big data is more data, coming faster, and with less structure • The “revolution” of mass data collection and of the Internet of Things • Storing data: from your computer to your network, to the cloud • Who owns data, who controls data?	Aberer
14:45 15:45 ☕	AI: understanding machine learning (ML) • Why is AI fashionable again (and what is ML)? • Out-of-the box examples: face recognition, text recognition, image labelling • A machine’s learning process: basic notions • Supervised vs. unsupervised learning • Learning in the lab vs. learning in the field • Overview of key techniques: neural networks (and deep learning), Bayesian statistics, decision trees (to be decided by teacher) • Which tasks is ML good at today? Which will it be tomorrow?	Aberer
16:00 17:00	Trust in social networks • Social networks as a global phenomenon • Using social network’s big data to learn about beneficiaries • The risks of using social network’s big data • Using social networks to engage with beneficiaries • “Fake news”: what can you trust? • State of the technology to detect fake news • Fake news factories as state-sponsored cyberwarfare	Aberer

Thursday, March 28: Machine Learning and Big Data

09:00 10:00 ☕	Biases • The impact of biased data in humanitarian action • Data with pre-existing biases • Biases in data collection • How analytics can emphasize biases • Identifying and correcting biased analytics • Does anonymization help fight biases, or does it make it harder? • Explaining the outcomes of AI	Troncoso
10:15 11:45	Privacy and Data Protection • Confidential data, personal data, sensitive data, with a specific focus on humanitarian scenarios • Techniques to make data “safe”: “anonymization”, de-identification (and re-identification), pseudonymization, hashing (and salting), aggregation, mashing, etc. • Why is anonymization hard, and what to do about it? • Privacy issues of metadata • The politics of privacy and the commercialization of data • Commercial and Government “big data surveillance”	Troncoso
11:45 12:45 🍕	Securing Data • How to identify personal data that is collected, generated or processed? • Understanding the threat model • Data minimization principles • Mitigation measures (and how to evaluate their effectiveness)	Troncoso
13:45 14:45	Digital trust implications of AI • Is it just data an alytics with fancy techniques (answer: no)? • ML as a specific vulnerability: faking data, influencing learning • How to protect ML processes?	Troncoso
14:45 15:15 ☕	Applying ICRC’s Data Protection Impact Assessment (DPIA) for data analytics and big data	Marelli
15:30 17:00	ML and data protection case study • Presentation of the scenario • Work in group	Aberer and Troncoso

Friday, March 29

Machine Learning and Big Data (continued)

09:00 10:30 ☕ 10:45 12:15 🍽	ML and data protection case study (continued) • Work in group: continues • Class discusses each group’s assessment	Aberer and Troncoso

Looking Forward

13:15 14:30 ☕	Trends in modern cryptography • The limits of “classical” cryptography • Gaining forward secrecy • Is quantum computing a crypto-killer (and what to do about it)? • Regaining trust in the cloud with homomorphic encryption • Case study on homomorphic encryption (hype of reality?)	Aumasson
14:45 16:00	Blockchains and smart contracts • Blockchain concepts: distributed ledger, co-authority, etc. • Balancing nonrepudiation with rectification, deletion, or objection • Smart contracts: the blockchain as a program • How much can you trust blockchains? • Private data on the blockchain: encryption and access control • Rectification, deletion, objection • Connecting the blockchain to the real world • Case study on blockchain (hype of reality?)	Aumasson
16:00 17:00	Wrap-up • Take home messages on digital trust today and tomorrow • Feedback on the course	Dubochet And Marelli