How would you like your Digital Future served: Huxley-Orwell-Kafka Dystopian Style or Digitally Responsible?

Panel

Jean-Henry Morin
University of Geneva – CUI
Switzerland
Jean-Henry.Morin@unige.ch

Anat Zeelim-Hovav
Korea University Business School
South Korea
anatzh@korea.ac.kr

David P. Maher
Intertrust Technologies
California, USA
dpm@intertrust.com

Yair Levy
Nova Southeastern University
Florida, USA
levyy@nova.edu

ABSTRACT

This panel brings together leading scientists and scholars in various areas of cybersecurity to initiate a discussion on a very controversial issue: shaping the digital future of our society. Digital Responsibility of different stakeholders is considered and debated arguing for an all-embracing consideration to broaden the scope of what is commonly known as Critical Infrastructure. Drawing on the panel participants and the audience, we hope to set the ground for agendas in research, industry, and public policy in an interactive part of the panel to be collected and documented after the panel.

Keywords: Critical Infrastructure, Security, Cybersecurity, IoT, Cloud, Digital Responsibility

PANEL OBJECTIVE

The objective of this panel is twofold. The first goal is to take a broader view at what Critical Infrastructure (CI) is in our increasingly digital society. Common definitions from industry and literature essentially refer to vital assets or systems essential for a society. While such a definition fits very well, we contend the scope of what it actually covers must be broadened to include the Internet of Things (IoT), cloud computing and other digital platforms massively used and commercialized to support our everyday activities. These infrastructures have become as critical for a sustainable and responsible digital society as water, energy, and transportation systems commonly known as CI. Recent events such as the October 2016 distributed denial-of-service (DDoS) attack against Dyn.com, which brought down the Internet for a large part of the US, IoT search engines such as Shodan.io opening doors to insecure IoT devices, Samsung televisions listening and recording conversations in our homes or more recent attempts in the Smart Toy industry potentially putting at risk our children with direct access to them in their bedrooms. Identifying and debunking the irresponsible stand of the industry and the key role of public policies in this context is essential to ensuring that we are not headed towards a dystopian digital future rehashing a poor blend of Huxley, Orwell and Kafka.

The second goal, based on a broader redefinition of CI, is to assess the role and the influence of three groups of stakeholders (i.e., industry, people, and public policy/state) on CI and subsequent implications for a responsible digital society. Specifically, we anticipate opening the panel to a collaborative session with the participants to identify key actions that must be undertaken for each stakeholder. This could set the ground for agendas in research, industry and public policy, and provide people with key evaluation criteria when consuming digital systems and services as well as ensuring that public policies are in place to support a digitally responsible and sustainable society.
Critical Infrastructure (CI) commonly refers to assets and systems having the mission of critical or vital requirements for society. These may range from traditional commodities such as water, energy, transportation systems, to finance, healthcare, security and defense infrastructure. We focus on three stakeholders within this ecosystem: (a) the industry providing these systems and services for profit; (b) governments, whose role is focused on designing the proper public policies for a society to evolve; and (c) the people, who largely depend on their governments to provide the proper frameworks for society and who consume what the industry provides them with. The three stakeholders including the overlaps of each are shown in Figure 1.

Increasingly, industry is pushing towards a democratization of connected devices and cloud-based services. As our societies rely more and more on such platforms, they have also become part of CI. However, industry could not care less about the security by design and privacy by default features essential to protect the users of such infrastructure, but focusing essentially on ensuring that these devices and services are sold as soon as possible. For example, recently, LG announced in South Korea that all of their home appliances will be IoT ready starting in 2017. Combining that with the Samsung Smart TV eavesdropping design, you can easily picture a “big brother” dystopia.

Governments have realized recently the potential impact of what is now commonly referred to as the 4th industrial revolution. Typically countries have taken different approaches to address, or ignore, the necessity of having a digital agenda. Some countries have formal digital agendas used as a basis for public policies, while other have capitulated on the issue leaving it to the market to figure out, or worse completely ignoring the issue. Countries with formal agendas have taken responsibility towards addressing the issue of a more sustainable digital society. Countries relying on market forces are handing over this responsibility to industry.

Given these two stakeholders, people are torn between convenience and a digitally responsible society. Hence, a potential gap exists between the people and their governments to the point one might even wonder whether there could be an untold agreement between industry and governments towards Huxley’s Brave New World dystopia.

---

1 http://m.pulsenews.co.kr/view.php?year=2016&no=765082
Panelists

- **Jean-Henry Morin**: Co-Moderator / Panelist, is a professor of Information Systems at the University of Geneva, Switzerland. He is a member of the Institute of Information Service Science and president of ThinkServices, a Geneva-based think (do) tank on Service Science and Innovation where ThinkData.ch was designed. Specialized in information security with a particular focus on Digital Rights Management in the enterprise and media sectors, his work on Exception Management in DRM Environments has been transferred to industry. His research areas are in socially responsible and sustainable security, cloud computing, Internet of Things, privacy, data protection and transparency. Author of numerous scientific publications, he recently published a book on Digital Responsibility (Editions Fyp, 2014) where he argues about the value of informed trust and transparency as the basis of an emerging principle of Co-Compliance (collaborative compliance).

- **Anat Zeelim-Hovav**: Co-Moderator / Panelist, is a full professor at Korea University Business School in Seoul, South Korea. Her research interests include the socio-technical aspects of organizational information security, risk assessment, innovation management, and Futures research. Professor Hovav has published in internationally refereed journals such as Information Systems Research (ISR), Information & Management, Communications of the ACM, Journal of Business Ethics, Research Policy, Computers & Security, Information Systems Journal (ISJ), Journal of Pervasive and Mobile Computing, International Journal of Project Management, Information Systems Management (ISM), Communications of AIS (CAIS), Information Systems Frontiers, and Risk Management and Insurance Review. Dr. Hovav is the winner of the 2013 Citation of Excellence Award. She has presented her work internationally in academic and industry conferences and workshops.

- **David P. Maher**: Panelist, has over 30 years of experience in secure computing and is responsible for Research and Development at Intertrust. Before joining Intertrust in 1999, he was chief scientist for AT&T Secure Communications Systems, Head of the Secure Systems Research Department, and security architect for AT&T’s Internet services platform. After joining Bell Labs in 1981, Maher developed secure communications, information vending, and e-commerce systems. He was Chief Architect for AT&T’s STU-III secure voice, data, and video products used by the White House and Department of Defense for top-secret communications. In 1992, Maher became a Bell Labs Fellow in recognition of his accomplishments in communications security. Maher holds multiple patents in secure computing; has published papers in the fields of mathematics and computer science; and has consulted with the National Science Foundation, National Security Agency, National Institute of Standards and Technology, and the Congressional Office of Technology Assessment. Maher holds a Ph.D. in mathematics from Lehigh University. He has taught electrical engineering, mathematics, and computer science at several institutions.

- **Yair Levy**: Panelist, is a professor of Information Systems and Cybersecurity, as well as head of the Information Assurance and Cybersecurity MS and Ph.D. programs at the College of Engineering and Computing (CEC), at Nova Southeastern University (NSU), Florida, USA. He heads the Levy CyLab, which conducts innovative research from the human-centric lens of four key research areas Cybersecurity, User-authentication, Privacy, and Skills (CUPS), as well as their interconnections. Author of numerous scientific publications, he is a reference in cybersecurity. He is an IEEE Senior Member, President of the AIS’ Special Interest Group on Information Security and Privacy, as well as ‘Lifetime Academic Achievement Award’. He has been an active member of the US Secret Service (USSS)’s - Miami Electronic Crimes Task Force (MECTF) and The South Florida Cybercrime Working Group (SFCWG). He was trained by the Federal Bureau of Investigation (FBI) on various topics, and actively serves as a member of the FBI/InfraGard, and consults federal agencies, state, and local government groups on cybersecurity topics. He is also a frequent invited keynote speaker at national and international meetings, as well as regular media interviews as a Subject Matter Expert (SME) on cybersecurity topics.