Safety in the Online World of the Future

Nadeem Douba, Björn Rütten, David Scheidl,
Paul Soble, and D'Arcy Walsh

> *"The errors of a theory are rarely found in what it asserts explicitly; they hide in what it ignores or tacitly assumes."*
>
> Daniel Kahneman
> Nobel Laureate in Economic Sciences (2002)

In this article, we address what it means to be safe in the online world of the future by advocating the perspective whereby improving safety will improve resilience in cyberspace. We adopt a specific approach towards transdisciplinarity; present a weakly transdisciplinary model of the safety context and an initial position about what existing disciplines are most relevant; and link prospect theory to risk-based decision making as one example that could lead to a new paradigm for safety. By treating safety as a transdisciplinary challenge, there is an opportunity to enable the participants of the online world to become more productive and creative than ever before. The beneficiary of this increased productivity and creativity will ultimately be the public. The perspective of this article is of interest to senior decision makers, policy makers, managers, educators, strategists, futurists, scientists, technologists, and others interested in shaping the online world of the future.

Introduction

This article focuses on the nature of safety in the future online world to enable humanity to reach profoundly new levels of productivity and creativity. Bailetti, Levesque, and Walsh (2014) envision an online world for 2030 that is safe (i.e., users communicate with accuracy and enduring confidence), productive (i.e., users make timely decisions that have an ongoing global effect), and creative (i.e., users can connect seemingly unrelated information online). Their proposed view is characterized by seven conditions of the future online world: i) global-scale autonomous learning systems; ii) humans co-working with machines; iii) human factors that are authentic and transferrable; iv) global scale whole-brain communities; v) foundational knowledge that is authentic and transferrable; vi) timely productive communication; and vii) continuous technological adaptation.

Key research questions pertaining to the safety characteristics of this future world include:

- Under what conditions does an attacker have an advantage over an infrastructure protector?
- Why do many infrastructure protectors and users not adopt effective mechanisms that provide safety and privacy?
- What are the resources, processes, and values to concurrently provide online safety and privacy to users?
- What are the characteristics of the individuals and organizations that are most likely to attack?
- What are the enhanced characteristics of safety through disclosure (i.e., by being open and not by being proprietary)?

If progress is made understanding the underlying properties of safety that are required to address these questions, then a foundation will be provided that promotes scientific progress and the arts within a society that is ever more connected on a global scale.

The Internet was not created to be safe but is being increasingly used in a way that requires that it be so. The increasing pervasiveness of cyber-based systems and infrastructure, and society's growing reliance on them, shifts the perspective concerning their proper opera-

Safety in the Online World of the Future

Nadeem Douba, Björn Rütten, David Scheidl, Paul Soble, and D'Arcy Walsh

tion from security to safety. Although defending networks and other information assets is necessary, it is part of the larger intent of securing these systems' ability to produce services and functions upon which society depends. Safety is often associated with unintended disruption, and security is often associated with intended disruption; both concepts affect the proper operation of cyber-based systems and infrastructure. Safety properties include security properties (Burns et al., 1992; Leveson, 2013; Young & Leveson, 2013). Safety is the foundation that promotes scientific progress and the arts within a society that is ever more connected on a global scale; it enables the global knowledge commons that is an engine of human progress.

This view of safety is sympathetic and compatible with the ultimate intent of copyright and patent laws. Article I of the American Constitution makes clear that the beneficiary of publications and inventions is the public – copyrights are granted and patents are issued in order "to promote the Progress of Science and useful Arts" (Menard, 2014). The thinking behind Article I is that prohibiting people from copying and selling someone else's original work should be time bound to strike an appropriate balance so that individuals and organizations have the means to further create original work but in a manner that the public can also benefit from this work in a timely fashion (Menard, 2014).

In this spirit, the concept of safety (including security) is not restricted to the protection and control of property, because ownership is a concept that can vary across social contexts. Instead, improving the safety of cyber-based systems and services focuses on the intended use of these systems. Further, safety must have enduring resilience where "cyber- [or online] resilience is about digital literacy at every level of the organization/society, distributed leadership, and a capacity to adapt in a networked and fast-changing digital ecosystem" (Rütten, 2010). Thus, there is a responsibility for safety that transcends the technological disciplines.

Based upon our knowledge and experience, current approaches toward safety and security do not make an explicit connection to productivity and creativity when contemplating the transdisciplinary aspects of the problem domain. These approaches emphasize preventing failure instead of enabling success. A new online paradigm that implies an environment that is safe regardless of how much you interact within it is necessary "to promote the Progress of Science and useful Arts" (Menard, 2014) in the future.

This article makes three contributions. First, it provides insight about a particular approach for addressing the global and transdisciplinary aspects that we believe characterize safety concerns of the online world of the future. Second, the article presents a weak transdisciplinary representation of the safety context and an initial position about what existing disciplines are most relevant. Third, by linking prospect theory to risk-based decision making within the domain of cyber-resilience, it provides an example to advance the idea of safety through online interactivity that could lead to a new paradigm for safety for the future online world.

The Safety Context is Global and Transdisciplinary

A safe online world must be created and maintained by stakeholders at multiple levels of society, which suggests that a more holistic view is required to define goals and engage participants rather than following separate approaches to the problem from distinct disciplines, which individually tend to address a subset of stakeholders. The concerns of these stakeholders are accommodated by treating relevant disciplines in a unified way. The concept of transdisciplinarity (Nicolescu, 2005), creating a unity of intellectual frameworks beyond the disciplinary perspectives (Jensenius, 2012), offers an approach for constructing a view of safety as a composition of collaborating disciplines that address the concerns of these stakeholders.

A distinction may be made between strong and weak transdisciplinarity. Strong transdisciplinarity envisions a total system of knowledge without stable boundaries between the disciplines. However, in the case of weak transdisciplinarity, traditional methods and logic can be applied. Here, we focus on weak transdisciplinarity, where a transdiscipline extends its action through coordination among disciplines at several levels of organization: the first, lowest level refers to "what exists now" (i.e., the world as it is; the empirical level), the second level refers to "what we are capable of doing" (i.e., it is composed mainly of technology disciplines; the capacity level), the third level refers to "what we want to do" (i.e., the normative level), and the fourth level refers to "what we should do" (i.e., the value level) (Max-Neef, 2005).

Thus, we do not treat safety as strictly disciplinary (specialization in isolation), multidisciplinary (no cooperation), pluridisciplinary (cooperation without coordination), or interdisciplinary (coordination from a higher-level concept), but instead we treat it as a coordination amongst all hierarchical levels.

Safety in the Online World of the Future

Nadeem Douba, Björn Rütten, David Scheidl, Paul Soble, and D'Arcy Walsh

In an effort to practice weak transdisciplinarity in a systematic manner as advocated by Max-Neef (2005), we have adopted a four-level organization model at the core of the safety context, and a set of high-level categories of knowledge that should be coordinated to achieve a safe online environment (Figure 1):

1. *Online world of the future:* speculates about the safe, productive, creative aspects that will drive the evolution of the online world, including the key conditions that will be met by the future world (see Bailetti et al., 2014).

2. S*trategy for making scientific progress and transfer of knowledge:* includes research questions, research methods and techniques, new disciplines, assessment of progress, and the transfer of knowledge through education and other means.

3. *Legal/ethical concerns:* includes issues related to privacy, security, intellectual property, regulation, disclosure, and human-machine interaction for the individual and collective good.

4. *Human sciences:* includes human behaviour, cognition, and social dynamics; how people think, how people interact, and how societies and groups behave; what people think, their beliefs and ideologies; cultural factors; and value systems.

5. *Technical understanding of the communication environment:* includes issues related to scientific understanding and technical aspects, including real-time, manifestation of phenomena within the online environment and the deployment of interconnected systems of systems.

6. *Related domain models:* concern the promotion of specific theories or concepts relevant to the domain, for example: the Cyber Game (information versus power); safety (unintended and intended disruption); economic models (public, private, club, common pooled resource); political science models; human behavior (decision making under risk, deception, intent); technical methods and techniques related to attack, attribution, forensics, and impact of compromise; and specific business models.

7. *Important topics:* include specific perspectives or "game changers" that represent current informed thinking about the domain (e.g., supply/value chain; duality of risk – opportunities, threats; adoption; disclosure, disruption).

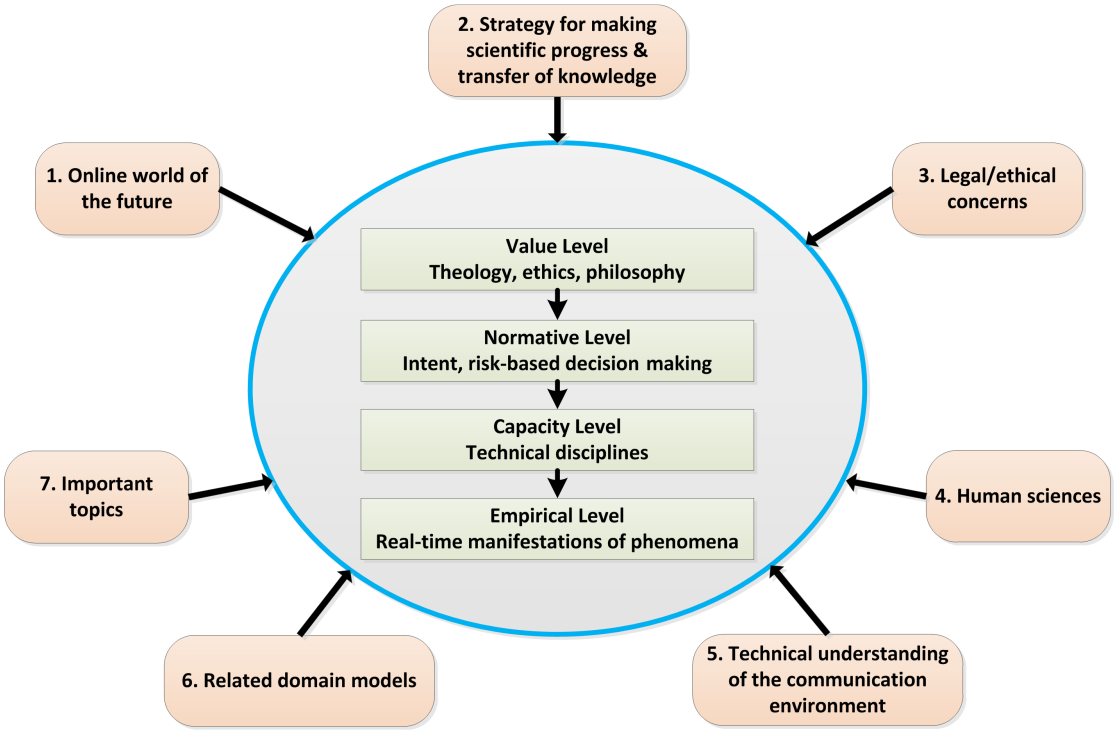

Figure 1. Four levels of concerns that need to be addressed to produce a safe online environment and seven categories of knowledge that influences the work done on these concerns.

Safety in the Online World of the Future

Nadeem Douba, Björn Rütten, David Scheidl, Paul Soble, and D'Arcy Walsh

Specific to the domain, we believe that the "Cyber Game" from the Global Cyber Game report (Tibbs, 2013) presents a useful domain analysis of the online world. The report was produced by the United Kingdom's Defence Academy, which provides education and training in a broad range of subjects – including command and staff, leadership, defence management, languages, acquisition and technology – for members of the UK Armed Forces and Defence Civil Servants. In delivering education and training, it is the Defence Academy's responsibility to prepare senior decision makers for the uncertainties and complexities of the challenges ahead. The report is a good example of this preparation as it pertains to the nature of cyberspace in the future, including cybersafety and cybersecurity.

The overall objective when producing the report was first to consider the broad question, "How should the cyber-domain be conceptualized?", and in the light of that question, to examine the implications for security strategy generally, the issues raised for state actors in the Internet age, new power relationships, possible sources and modes of future conflict, and the steps that need to be taken to prepare for a range of plausible possibilities (Tibbs, 2013).

The report examines these issues, in part, by proposing the idea of the Global Cyber Game as a framework that can be used for practical thinking about cyber strategy. Cyberpower and cybersecurity are conceptualized using a "Cyber Gameboard", which consists of a nine-cell grid. The horizontal direction on the grid is divided into three columns representing aspects of cyber-information: connection, computation, and cognition. The vertical direction on the grid is divided into three rows representing types of power: coercion, co-option, and cooperation. The nine cells of the grid represent all the possible combinations of power and information, that is, forms of cyberpower (Tibbs, 2013).

The central ideological decision of the Cyber Game is whether to play the game as if freedom of information content is a public good in itself or whether extensive control of information content is necessary for public safety (Tibbs, 2013).

Thus, the Cyber Game gives precedence to the concepts of information and power and the interrelationships that can arise when these two concepts are applied together. The Cyber Gameboard is a concise but powerful representation that permits reasoning about many of the aspects and complex interactions of cyberspace to achieve an outcome that can be successful despite, for example, known ideological conflicts, politics, and human nature whose complexity requires coordinated action.

The power dimension of the Cyber Game privileges the sub-concepts of cooperation (integrative social power), co-option (economic exchange power), and coercion (destructive hard power) as means to exercise power. On this dimension, cyberspace is a tool similar to new technologies such as airpower or net-centric warfare used to achieve effects on geopolitical actors with its own characteristics of power transition versus power diffusion.

The information dimension of the Cyber Game privileges the sub-concepts of connection (the physical data-handling domain), computation (the virtual interactivity domain), and cognition (the knowledge and meaning domain). On this dimension, an example bridging the gap from cyberspace to physical space is the Stuxnet case study of a cyber attack strategy to bridge connection, computation and cognition spaces (Kushner, 2013).

A Weak Transdisciplinary Representation of the Safety Context

This section introduces a weak transdisciplinary representation of the safety context of cyberspace and an initial position about what existing disciplines are most relevant. Because we lack a methodology for applying weak transdisciplinarity, our approach is based on our subjective confidence.

Figure 2 presents Cyber Game concepts and related disciplines using the four-level organizational model, including connections that cascade from the Value Level, through the Normative and Capacity Levels, to the Empirical level to indicate the coordination that must happen across levels amongst those concepts that are linked. Although the structure does not directly answer questions such as "What does it mean to be safe?" or "Who is safe from whom or what?", it unifies the elements that must be adjusted to evolve from the present situation toward the preferable future (Bailetti et al., 2014) in a way that addresses the multi-level complexity of the problem.

What we should do is addressed at the Value Level of Figure 2, including theology, values, security and privacy, intellectual property, regulation, disclosure, and the individual and collective good as they relate to human–machine interaction. Practical solutions must in-

Safety in the Online World of the Future

Nadeem Douba, Björn Rütten, David Scheidl, Paul Soble, and D'Arcy Walsh

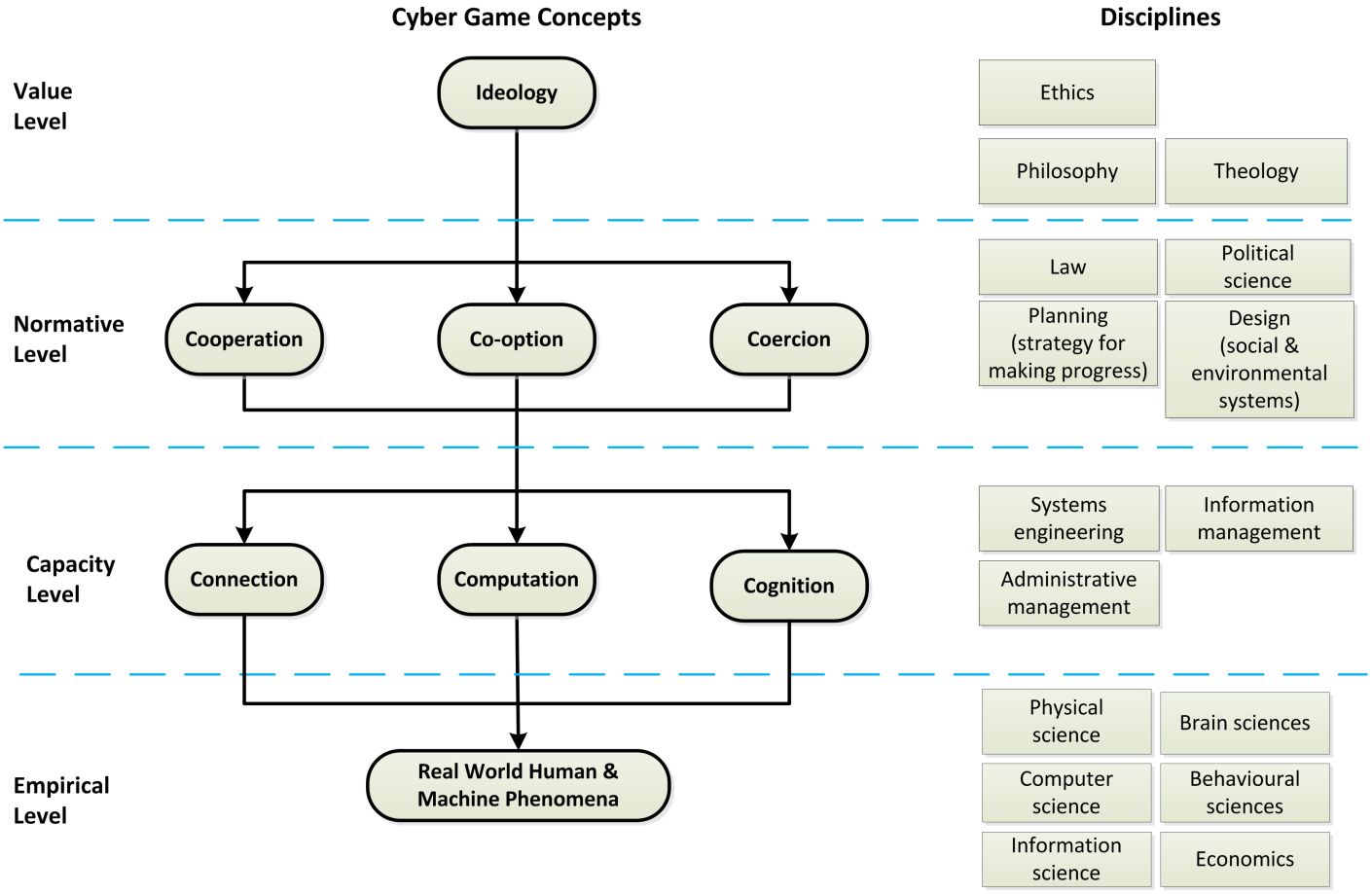

Figure 2. Cyber Game concepts and related disciplines categorized using the four-level model

volve this level to account for online participants who do not share the same views of such things as values, religion, and ethics.

What we want to do is addressed at the Normative Level of the figure, including risk-based decision making, management and planning, the strategy for making scientific progress and knowledge sharing, legal, and political concerns. We have also positioned the power dimension of the Cyber Game sub-concepts of cooperation (integrative social power), co-option (economic exchange power), and coercion (destructive hard power) at this level.

What we are capable of doing (composed mainly of technology disciplines) is addressed at the Capacity Level of the figure, including the information dimension of the Cyber Game sub-concepts of connection (physical data handling domain), computation (virtual interactivity domain), and cognition (knowledge and meaning domain).

What exists now (the world as it is) is addressed at the Empirical Level of the figure, including physical sciences, computer science, information science, brain sciences, and behavioural and social sciences.

The weak transdisciplinary model is a representation of the safety context of cyberspace. Relevant disciplines are identified at every level and these disciplines must be coordinated to achieve the safety goal in the face of the real-world complexities and conflicts.

Safety through Online Interactivity

This section provides an example of relevant disciplines that are coordinated to achieve safety by linking prospect theory to risk-based decision making in the con-

Safety in the Online World of the Future

Nadeem Douba, Björn Rütten, David Scheidl, Paul Soble, and D'Arcy Walsh

text of cyber-resilience. An important consequence of the example is the notion of safety through online interactivity.

The concept of cyber-resilience (Rütten, 2010) is addressed by Collier and colleagues (2014), who focus on the ability to prepare for and recover quickly from both known and unknown threats. They recommend linking technical data with decision analysis in an adaptable framework to move toward systems that are more resilient to dynamic threats by incorporating decision analysis methods and techniques "to accommodate value-centric perspectives inherent in multiple stakeholder views when addressing the challenge of establishing risk-based standards that will protect the cyber domain" (Collier et al., 2014). This approach is an example of weak transdisciplinarity.

Now consider prospect theory, which is the foundation of the field of behavioural economics. As an evolution of concepts that originate from statistics, economics, and psychology, it is another example that transcends a particular discipline. Using the concept of a reference point to indicate that the human response to losses is stronger than the response to corresponding gains (loss aversion) together with the concept of diminishing sensitivity, it is a coherent theory that can describe decision under risk: prospect theory provides a plausible way to describe different attitudes to risk for gains (as favourable prospects) and losses (as unfavourable propects) (Kahneman, 2011).

Prospect theory should be investigated as at least a partial theoretical grounding of risk-based decision making within the domain of cyber-resilience. It would contribute to descriptions of the behavioural aspects when humans are confronted with decisions "to prepare for and recover quickly from both known and unknown threats". Based on prospect theory, risk-based standards could be enhanced to better align with the decisions humans actually make under such circumstances.

Further, because prospect theory accommodates favourable as well as unfavourable prospects, we believe it applies beyond "risk-based standards that will protect the cyber domain'' (Kahneman, 2011). By accommodating both kinds of prospects, prospect theory in effect could also be considered a theory of decision making pertaining to the duality of risk, which treats each risk situation not just as a threat (an unfavourable propect) but also as an opportunity (a favourable prospect).

As an example from the medical domain (Kahneman, 2011), consider anesthesiologists, who benefit from feedback because their actions are quickly evident, and radiologists, who obtain less immediate information about the accuracy of their diagnoses. In both cases, risk can be considered as the difference between life and death. Saving a patient is an example of a favourable prospect and not saving a patient is an example of an unfavourable prospect. Anesthesiologists and radiologists become better at their profession as they save or do not save patients by continually making decisions under risk and learning and adapting (by modifying their protocol of intervention). Under very different circumstances, both kinds of medical experts must overcome their subjective confidence and must continually know the limits of their expertise as they become more experienced and knowledgeable.

In the context of cyber-resilience, viewing risk as an opportunity is a way to facilitate productive and creative outcomes within a society that is ever more connected on a global scale. When risk as an opportunity is applied within an adaptive learning framework such as the one promoted by Collier and colleagues (2014), online safety becomes a function of user online interactivity. Humans (providing insight and understanding) and systems/networks (interpreting information at scale) will interwork to assess and to achieve joint goals to predict continuously emerging complex phenomena (Bailetti et al., 2014). If such an environment existed, it would make a profound contribution in promoting the future "Progress of Science and useful Arts" (Menard, 2014): cyber-resilience in this sense is not just recovering from individual loss events, but more akin to reduction of brittleness in the protective measures (through an adaptive learning approach).

Conclusion

We presented an approach for addressing safety concerns in the online world of the future using a weak transdisciplinary model, including an initial position about what existing disciplines are most relevant. Although the model does not directly answer key research questions pertaining to underlying safety properties, it does provide a unified structure that accommodates the participation of stakeholders at multiple levels of society and a holistic view.

Instead of restricting the concept of safety (including security) to the protection and control of property, we emphasize improving the safety of cyber-based systems and focus on the intended use of these

Safety in the Online World of the Future

Nadeem Douba, Björn Rütten, David Scheidl, Paul Soble, and D'Arcy Walsh

systems that could lead to profoundly new levels of productivity and creativity for the benefit of society as a whole.

In order to make progress in understanding the underlying properties of safety, and to evolve from the present situation toward the preferable future (Bailetti et al., 2014), attention should be given to applying a methodology of transdisciplinarity that exclusively concentrates on joint problem solving of key research questions pertaining to the science–technology–society triad implied by the weakly transdisciplinary model that was presented. The investigation of prospect theory as a theoretical grounding of risk-based decision making within the domain of cyber-resilience is an example.

We foresee the possibility of a new online environment that becomes progressively safer for participants the more that online interactions occur within the environment. The idea is that a participant's fingerprint is enriched the more that the participant interacts online. The more enriched a participant's fingerprint becomes, the greater the potential for ensuring the safety of the participant. At the same time, the more a participant interacts online, the more opportunity there will be for the participant to be productive and creative.

With this perspective in mind, we believe that future work should contemplate both the productivity and creativity domains in depth to better understand how their respective underlying properties relate to safety when safety is a function of interactivity.

About the Authors

Nadeem Douba is the founding principal of Red Canari, an information security consulting firm that specializes in the areas of information technology and cybersecurity. With over 15 years experience, Nadeem provides consulting and training services for organizations within the public and private sector. He has also presented at some of the world's largest security conferences and is the author of many well-known open source security tools, including one used by the Internet Archive project. His primary research interests include open source intelligence, application and operating system security, and big data. He received his BEng in Systems and Computer Engineering from Carleton University in Ottawa, Canada.

Björn Rütten is the Senior Research Associate for National Security and Public Safety with The Conference Board of Canada. Bjorn leads the Conference Board's research projects in the area of national security and public safety and is responsible for the development and execution of the research plan of the Centre for National Security. He also contributes to other security-related network and research initiatives, such as those of the Centre for the North.

David Scheidl is a recent graduate from the Global Politics program at Carleton University in Ottawa, Canada. During his studies, he focused on security intelligence and geopolitics, with special emphasis on Western security agencies in both the cybersecurity and real-world intelligence fields. He has extensive background in military communications, having served in the Army Signals Reserve since 2009.

Paul Soble is a Science Advisor at the Communications Security Establishment (CSE) in Ottawa, Canada. Over the past three decades, he has held a variety of positions at CSE in the areas of enterprise architecture, visualization and data mining, speech and text natural language processing, adaptive antenna arrays, and systems development. He received his BSc and MSc degrees in Electrical Engineering from University of Manitoba in Winnipeg, Canada, and he is a licensed professional engineer in the province of Ontario.

D'Arcy Walsh is a Science Advisor at the Communications Security Establishment (CSE) in Ottawa, Canada. His research interests include software-engineering methods and techniques that support the development and deployment of dynamic systems, including dynamic languages, dynamic configuration, context-aware systems, and autonomic and autonomous systems. He received his BAH from Queen's University in Kingston, Canada, and he received his BCS, his MCS, and his PhD in Computer Science from Carleton University in Ottawa, Canada.

Safety in the Online World of the Future

Nadeem Douba, Björn Rütten, David Scheidl, Paul Soble, and D'Arcy Walsh

References

Bailetti, T., Levesque, R., & Walsh, D. 2014. The Online World of the Future: Safe, Productive, and Creative. *Technology Innovation Management Review,* 4(10): 5–12. http://timreview.ca/article/834.

Burns, A., McDermid, J., & Dobson, J. 1992. On the Meaning of Safety and Security. *The Computer Journal*, 35(1): 3-15. http://dx.doi.org/10.1093/comjnl/35.1.3

Collier, Z. A., DiMase, D., Walters, S., Tehranipoor, M. M., Lambert, J. H., & Linkov, I. 2014. Cybersecurity Standards: Managing Risk and Creating Resilience. *IEEE Computer,* 47(9): 70-76. http://dx.doi.org/10.1109/MC.2013.448

Jensenius, A. 2012. Disciplinarities: Intra, Cross, Multi, Inter, Trans. ARJ.no. Accessed November 15, 2014. http://www.arj.no/2012/03/

Kahneman, D. 2011. *Thinking, Fast and Slow*. Toronto: DoubleDay Canada.

Kushner, D. 2013. The Real Story of Stuxnet. *IEEE Spectrum,* February 26. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Leveson, N. 2013. *Engineering a Safer World*. Cambridge, MA: MIT Press.

Menand, L. 2014. Crooner in Rights Spat: Are Copyright Laws Too Strict? *The New Yorker,* October 20, 2014. http://www.newyorker.com/magazine/2014/10/20/crooner-rights-spat

Max-Neef, M. A. 2005. Foundations of Transdisciplinarity. *Ecological Economics*, 53(1): 5-16. http://dx.doi.org/10.1016/j.ecolecon.2005.01.014

Nicolescu, B. 2005. Transdisciplinarity – Past, Present, and Future. Il Congresso Mundial de Transdisciplinaridade, 6-12 September, 2005, Brazil. http://cetrans.com.br/textos/transdisciplinarity-past-present-and-future.pdf

Rütten, B. 2010. *Digital Ecosystem Resilience*. Ottawa: The Conference Board of Canada.

Tibbs, H. 2013. *The Global Cyber Game: The Defence Academy Cyber Inquiry Report*. Swindon, UK: Defence Academy of the United Kingdom.

Young, W., & Leveson, N. 2013. System Thinking for Safety and Security. *Proceedings of the 2013 Annual Computer Security Applications Conference (ACSAC 2013).*

Citation: Douba, N., Rütten, B., Scheidl, D., Soble, P., & Walsh, D. 2014. Safety in the Online World of the Future. *Technology Innovation Management Review*, 4(11): 41–48. http://timreview.ca/article/849

Keywords: safety, security, cybersecurity, weak transdisciplinary, prospect theory, risk-based decision making