Chapter 6
Making Sense of Cybersecurity in Emerging Technology Areas

Claire Vishik, Intel Corporation
Michael Huth, Imperial College London
Lawrence John, Analytic Services (ANSER)
Marcello Balduccini, St. Joseph's University

1. Abstract

Shortening technology development cycles in ICT (Information & Communication Technology) make it imperative to anticipate the emergence and evolution of new computing technologies and ecosystems. A wide range of questions must be answered to ensure that new technology environments are viable, including the examination of usability, efficiency, usage models, security, and privacy. These contextual aspects of new technologies are essential for their adoption. They are also important to understanding the potential of new types of cybercrime and requirements for the development of mitigation techniques. However, we lack methodologies to model and predict the features of the evolving ICT ecosystems and the requirements their evolution places on legal systems and regulatory frameworks. The absence of such models is a significant obstacle to creating consistent approaches necessary to forecast both the technology development and the trends in cybercrime.

We discuss which potential methodologies could be used for forecasting cybersecurity concerns in disruptive technology areas and trends in cybercrime in complex environments. We believe a unified approach should be developed for predicting cybersecurity effects of innovative technologies and trends in cybercrime. We first examine concepts associated with emerging technologies and their impact on cybersecurity. We then look at approaches to modelling and analysis already developed in adjacent spaces, with focus on knowledge representation and risk engineering, and analyse representative examples to illustrate the benefits these approaches can bring.

2. Technology Forecasting and Innovation

2.1 Methodology for predicting trends in cybersecurity

The term "technology" can denote products and services developed based on scientific and engineering knowledge, but it may also refer to related knowledge and its integration to solve complex application problems (see NIC 2016). Attempts to anticipate emerging technology areas and their impact are made routinely in the fields of policy, market analysis, research funding, and many more. Investments and policy decisions are made in anticipation of predicted developments. Research in the "disruptiveness" of new technologies may focus on the disruption of markets by innovation as in (Govindarajan and Kopalle 2006) or, more frequently, on softer metrics, attempting to forecast future trends based on past evolution, statistics, or superficially logical considerations.

Such forecasts are rarely perfect, but they allow the broad community to define an area of focus for innovation. For example, in the United States, high-level research priorities in cybersecurity

were established and tracked for a number of years, providing a relatively stable set of potentially disruptive technologies in cybersecurity and vocabulary for defining them.[1] The resulting report divides potentially disruptive technologies into several descriptive areas, e.g., "moving target defence" and "security of cyber-physical systems," and associates them with process-oriented activities, such as designed-in security, the establishment of scientific foundations of cybersecurity, or transition to practice. Although the resulting framework does not reliably forecast future technology environments, it allows us to talk about technology innovation and its influence on trends in cybercrime consistently when faced with cyberattacks of ever-increasing speed and scale. Can we do better than that? Below, we suggest approaches and provide examples to improve forecasts for disruptions in cybersecurity and for the evolution of cybercrime.

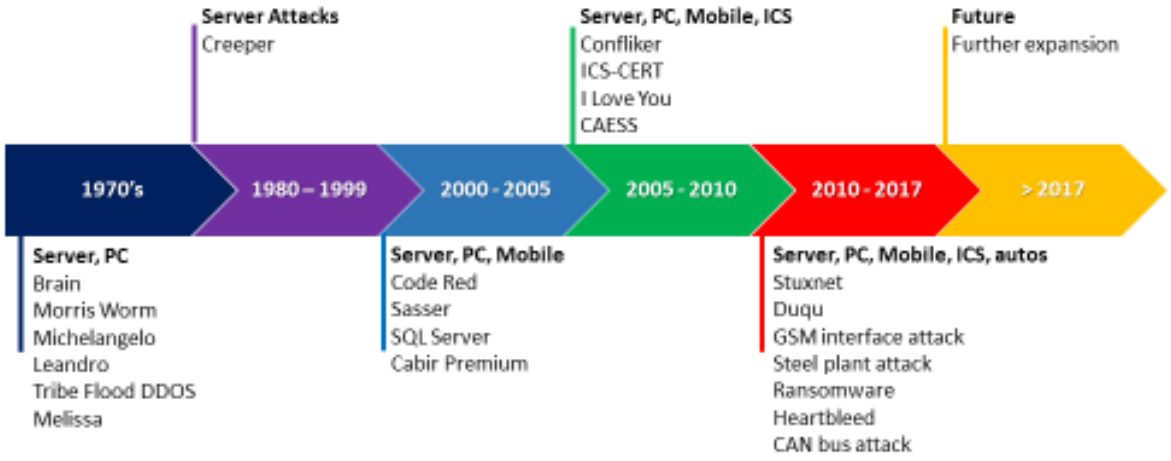

Figure 1. Evolution of cyberattacks: The types of systems vulnerable to cyberattack have changed as technology and adversary methods have progressed.

To understand the impact of emerging technologies on cybersecurity more accurately, we need a more formal and multi-disciplinary approach. Traditionally, "technology foresight" (Van Zwanenberg *et al.* 2009) is a structured activity, in which new possibilities of technological innovation are examined with a view toward harnessing the greatest economic or social value of future "technology assessment". Van Zwanenberg *et al.* focus on predicting the impacts of technology as used by humans (foresight) and on creating methodologies to inform the selection and deployment of technology (assessment). These two approaches, foresight and assessment, are often combined to yield "strategic intelligence" (Kuhlmann *et al.* 1999). In the real world, planners frequently must think in terms of decades (foresight), but might also need to introduce new technology in the short- to medium- term (assessment). In increasingly smart cities, cybersecurity and crime are important aspects in both foresight and assessment activities.

In fast-emerging areas, where new threats, threat vectors, attack methods, and defensive capabilities emerge daily, it is a challenge to link these developments to cybersecurity and cybercrime. However, it is not a bleak picture, and, as we discuss later, second-order predictions, such as trends in cybersecurity, are somewhat easier to capture. Forecasting of longer-term technology trends has been shown to be no better than random selection of possibilities, unless a low baseline is taken, focusing on obvious requirements (Quinn 1967). Views such as "security will continue to be important in electronic commerce" are likely to be correct, but they are obvious. We may not be able to anticipate even the *types* of technology

that will exist at some future point, but some techniques could increase the likelihood of an actionable answer. Making well-founded assumptions about the technology environment in general makes it easier to predict impacts on the cybersecurity of citizens, systems, or entire infrastructures.

Cybersecurity and trends in cybercrime are typically secondary impacts of the introduction of innovative technologies; they can be addressed with greater confidence than predictions for technology evolution in general. To illustrate, a prediction that flying autonomous vehicles will become common in twenty years (see NASA 2017) may be justified based on evolution of the technology up to now. But a more concrete prediction that 30% of new vehicles sold will be flying autonomous vehicles is hard to justify based on known technology and business trends. We lack scientific techniques to assess the probability of such a prediction. However, we have greater knowledge about the evolution of known cybersecurity and privacy threats, and vulnerabilities for flying autonomous vehicles based on what is known today. Although incomplete, this secondary assessment of cybersecurity could be more reliable than a more concrete technology prediction, because the secondary impacts of new technologies are more stable and depend more on the general technology environment than primary disruptive technologies.

2.2 Possible techniques for prediction of future technology

Let us consider specific techniques that can help anticipate cybersecurity and privacy concerns for innovative technologies with unknown usage models and evolution paths. How can we make sense of cybersecurity issues for technology environments that are too novel to be well understood or still evolving? Several approaches from adjacent research areas are available.

1. **Analysis based on past behaviours in similar environments**. This approach permits a reasonably reliable core assessment based on known facts and techniques, but does not offer structured methodologies to extract novel components and problems.

Studying past disruptive technological innovations may help us better understand how future disruptions or emerging technology with disruptive potential may influence the technological fabric that underpins modern societies and economies. As an example, the U.S government spent $1.5 billion in the late 1950s on developing a high-altitude strategic bomber, the XB-70 Valkyrie. However, the emergence of surface-to-air missiles that could reach high altitudes led to swift cancellation of the project and a complete change in U.S. tactics. This apparent failure fostered research that created innovations in low observable design and coatings, greatly reducing the effectiveness of the aforementioned missile technology innovation (Rao & Mahulikar 2002). The Cold War environment did not exhibit either wide diffusion of emerging technology or capabilities analogous to current and emerging cybersecurity threats. It does not, therefore, qualify as a sufficiently similar environment. We must look to more recent use cases for guidance.

With regard to modern developments, such as Bitcoin (Nakamoto 2008) and blockchain technology, analysis based on past trends could point to expansion to other areas requiring robust transaction records for auditing or operations. Aerospace, automotive, and supply chains, amongst others, could use blockchain and experience privacy and security issues detected for Bitcoin systems. We may suppose that sectors where blockchain is likely to be used will experience cybercrime trends informed by those detected for Bitcoin and/or for new sectors of blockchain use – with the necessary adjustment for new technology.

2. **Examining and combining analyses from different stakeholders**. This approach permits incorporation of societal and economic considerations, but can be imprecise.

The interpretation of the impact of technologies is partly a function of the objectives for the forecasting activity and the expertise of those who conduct it. Governments are interested in impacts on their societies and economies, including national security. International enterprises focus on financial impacts, their technological competitiveness, and impacts on trade and business models. Individuals are concerned with the impacts of emergent technology on their personal life and standard of living, in areas like food safety, online security, protection of personal data, and job prospects. Different technologies and stakeholders operate within different time horizons and tolerate different risks. In infrastructure-heavy sectors, such as telecommunications or manufacturing, longer-term analysis is needed than in areas such as software or consumer electronics, where planning horizons are shorter. In some areas, such as cyber-physical systems, time horizons vary between a lifespan of a few minutes (one-use medical sensors) and several decades (industrial control systems). But the essential technologies in these two areas are similar, leading to the need to develop models capable of evaluating both paradigms in one framework.

Continuing our blockchain example, examination of cybersecurity threats from different market and government sectors in which blockchain is used can help anticipate some of the cybersecurity vulnerabilities that are likely to be important, and apply already known or newly created mitigation techniques.

3. **Collecting "signals" from the environment and analyzing their impact.** Signals can include diverse evidence of evolving characteristics of the technology environment, job advertisements, information on acquisition and alliances, research publications, and many other elements. The success of this approach depends heavily on the data quality and interpretation of these signals.

By collecting meaningful information over time on a wide range of topics, consistent trends can be constructed, including for cybersecurity. Although conclusions may not be immediately actionable, they can be improved by refining methods of signal interpretation. Artificial Intelligence techniques could be added to this methodology, potentially offering deep or unusual insights into current and future trends.

To illustrate, signals and data from currently active blockchain markets and analysis of those signals could provide a practical, sometimes quantitative, foundation for more theoretical assumptions on the vulnerabilities of future blockchain systems described for the first two approaches.

4. **Creating models of disruptive technologies**. Insights and results depend on the quality of the model and the viability of its assumptions, but they permit generalization of the methodology and evaluation of multiple scenarios.

Emergent technology may be disruptive in several ways. Innovation can make past technology obsolete, diminishing returns on prior investments. Or it can challenge past business models, including the rationale for existing service or product platforms; note that none of the larger companies that produced computers based on analogue transistors survived the transition to digital transistors. Disruptions may also have important second order effects. For example, if

almost all cars are both powered by electricity and fully autonomous, opportunities for energy savings through coordinated road usage and planned recharging may increase; however, this may increase preference for cars over public transportation, potentially increasing energy demands (see NIC 2016). Such insights can be refined through modelling and can assist theory development not only for the primary environment (autonomous cars), but also for emerging cybersecurity and privacy concerns in an environment with predominantly autonomous vehicles.

Continuing our blockchain example, insights gleaned from approaches 1-3 (two theoretical approaches and one data-driven validation mechanism) are likely to provide enough useful information and strong assumptions to shape a model of blockchain-enabled environment. In such a model we can explore different use cases within a single framework, to enable examination of future impacts on cybersecurity and privacy and trends in cybercrime for this space.

5. **Ontology[2]-based analysis**. Knowledge engineering[3] techniques can support structured analysis of components of innovative environments. They can also enable reasoning about the relationships within these environments; finding hidden connections and constraints; and understanding how the same technology can be used for different scenarios, ranging from digital business and e-government to cybercrime.

The intrinsic complexity of modern technology environments makes it hard to understand how innovative elements impact other environments and technology users. Traditional approaches provide silo-based analysis, but, without finding hidden connections, we cannot assess hypothetical situations that do not yet exist or have not yet been detected. What cybercriminal threats are there for a passenger in a flying autonomous vehicle? How can an old public ledger affect the security of an account created twenty years later? Reasoning algorithms in ontologies can help find answers to these questions.

Returning to blockchain, an ontology and its reasoning engine can draw from the techniques described earlier, while highlighting implicit relationships and constraints not noticed before. We may thus identify a lack of alignment between requirements in regulatory frameworks in some areas (e.g., aerospace) and capabilities of blockchain systems or their potential ability to protect against or create the foundations for certain types of cybercrime.

2.3 Trend forecasting and cybercrime

The connection between innovative technologies and novel opportunities for cybercrime should be understood using a number of approaches. Because cybercrime covers a wide range of activities where information technology facilitates criminal purposes, the connection between the new technologies and the new forms of cybercrime is important. The same ecosystems are used for digital business and by cyber-criminals (Kraemer-Mbula *et al.* 2013). Thus, a better understanding of emerging technologies and business models should also lead to a better potential to anticipate mitigations for cybercrime.

Quantum Computing and Post-Quantum Cryptography provide an example of the connection of emerging technologies and new types of cyber threats, and, consequently, cybercrime. The ability of Quantum Computing (Shor 1995) to potentially compromise existing digital signature solutions suggests that emergent technologies may not only threaten the cybersecurity of present systems, but may compromise the integrity of past commercial or legal transactions, potentially damaging the trustworthiness vital to a nation's social contract. Digital

signatures and authentication enabled by asymmetric cryptography rely on the fundamental assumption that only a signatory can produce a signature while anyone can verify it. For this assumption to hold, the task of synthesizing a signing key from a verification key and a message must be too complex to perform in any reasonable amount of time by a state-of-the-art computer. Thus, these schemes are particularly vulnerable in a Quantum Computing environment. To make things worse, they are as pervasively used as asymmetric cryptographic algorithms for data encryption. The emerging problem with this technology is widely known, providing additional time and opportunities for cybercriminals to develop new techniques.

When fundamental changes in a paradigm are envisioned, as in Post-Quantum Cryptography (Bernstein 2009), ontological analysis can identify impacts on complex systems or legal and regulatory environments. Extending this example to blockchain, ontological views of blockchain systems and Post-Quantum Cryptography, informed by the outcomes of other forms of analysis, permit the developers to better understand the effect of fully functional quantum computers on blockchain systems and the effect of this paradigm change on cybercrime.

To summarize, we cannot rely on proven approaches to identify and analyse emerging technology environments and their cybersecurity and privacy properties. But cybersecurity and privacy threats and vulnerabilities identified for older, yet similar, environments can be a useful guide because they represent derivative rather than primary insights. A number of techniques could improve the outcomes for anticipating disruptive technologies; an aggregation of these methodologies can improve the outlook.

2.4 Disruptive technology and regulatory frameworks

New technology environments have a profound effect on the efficacy and content of regulatory and legal frameworks, which are also influenced by the need to combat cybercrime. However, this influence is delayed. Consider the evolution of the concept of anonymity in the modern technology environment. Anonymity is an important foundation for privacy and data protection, but the ability to achieve relative anonymity online is also an enabler of cybercrime.

Anonymity has gained importance largely due to European legislation on personal data protection. Anonymous data are not “personal data” and therefore are outside the field of application of, e.g., the EU General Data Protection Regulation.[4] But is anonymity absolute? It cannot be in some contexts. A writer can be anonymous to readers, but not to the publisher. The multifaceted nature of anonymity is much more prominent in modern digital contexts.

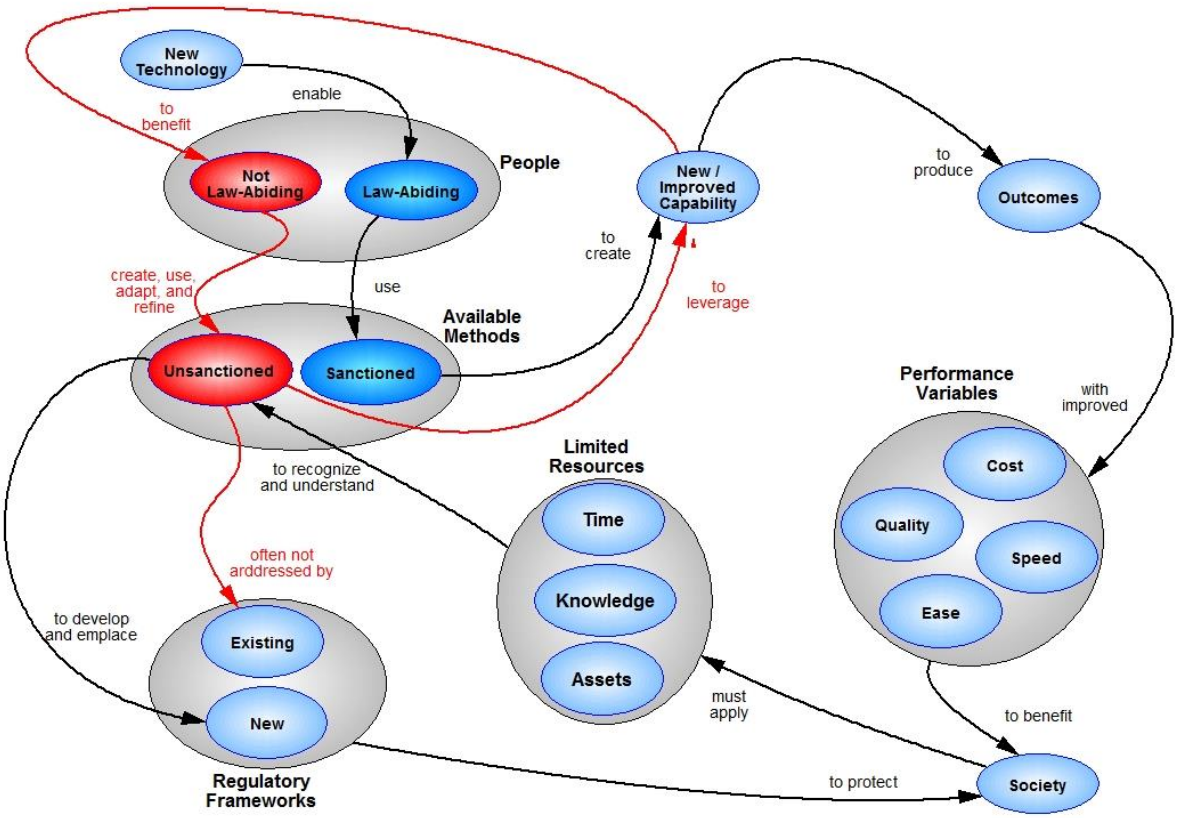

Figure 2. Cybercriminals and the law: This simplified systemigram illustrates how cybercriminals can get and remain ahead of cybersecurity regulatory frameworks.

Data can be considered personal if a data subject is identifiable. The subject need not be directly identified, but can be identifiable in principle, for instance, through aggregation of data sources. As the number of potentially related data sources and diverse identifiers increases, the ability to re-identify a user through multiple data sources also grows. EU regulators adopted[5] the idea of 'reasonableness' as a foundation for the establishment of whether the data should be considered personal or anonymous. The reasonableness test relies on the amount on effort needed to re-identify a data subject[6].

However, the complexity of the digital processes is likely to lead to further dilution of the strict definition of anonymity. It will become more difficult to interpret issues related to autonomy in the context of the latest technologies: for example, determining the appropriate level of anonymity within distributed ledgers or whether the distributed nature of many blockchain systems could violate requirements for, and place restrictions on, international data flows. In consequence, legal and regulatory approaches require continuing evaluation and modification of requirements to match the computing environment. It will also be necessary to reconcile, via technology adjustment and regulatory actions, the need to avoid re-identification to support data protection for users with the need to trace and combat cybercrime.

2.5 Disruptive technology and threat landscapes

A disruptive technology could dramatically change the cybersecurity threat landscape, yield effective new countermeasures against cybersecurity attacks, or influence the ecosystem in which cybersecurity attacks are realized and monetized. For example, the invention of Bitcoin (Nakamoto 2008, Narayanan *et al.* 2016) has the potential to make the flow of financial assets traceable, making it harder for cybercriminals to act through a combination of social and cyber-attacks. But the pseudo-anonymity that Bitcoin affords to its users raises the interest of

cybercriminals in Bitcoin transactions because such transactions may be hard to connect to legal actors. However, intelligent data analysis allows for the identification of particular Bitcoin users or operators of its clusters (Meiklejohn *et al.* 2016). This is an innovative environment with some features not previously encountered. The assessment of its impact on cybersecurity must draw from techniques described above to be comprehensive and reasonably pragmatic. Similarly to anonymity, the legal and regulatory aspects of cybersecurity with regard to blockchain-enabled environments are expected to gradually evolve, as will the regulatory frameworks for virtual currencies. Society will have to anticipate and resolve a range of issues as new technologies take hold, such as the use of blockchain-based cryptocurrencies for cybercrime.

Anticipating gradual evolution of technology is easier than guessing the fundamentally new directions of distinctive innovations such as a digital transistor or software-defined radio, because incremental processes founded on known principles are easier to capture. However, it is important to understand that, while technology disruption through incremental change may be less opaque to researchers, in some situations secondary properties with regard to cybersecurity and privacy may abruptly lose their incremental nature. Thus, gradual change in the general technology environment may lead to abrupt deterioration or improvement in security, limiting the usefulness of analytical tools developed to reflect an earlier state of a similar technology environment. To overcome consequences of abrupt changes resulting from originally incremental developments, good quality metrics and advanced risk models may be leveraged.

We illustrate such gradual improvement in the use of military-grade GPS systems. The evolution of the features of the technology was obvious in military systems. But when GPS technologies became mature enough and cheap enough to support mass location services on non-dedicated devices, security and privacy concerns associated with location tracking emerged, requiring a separate solution.

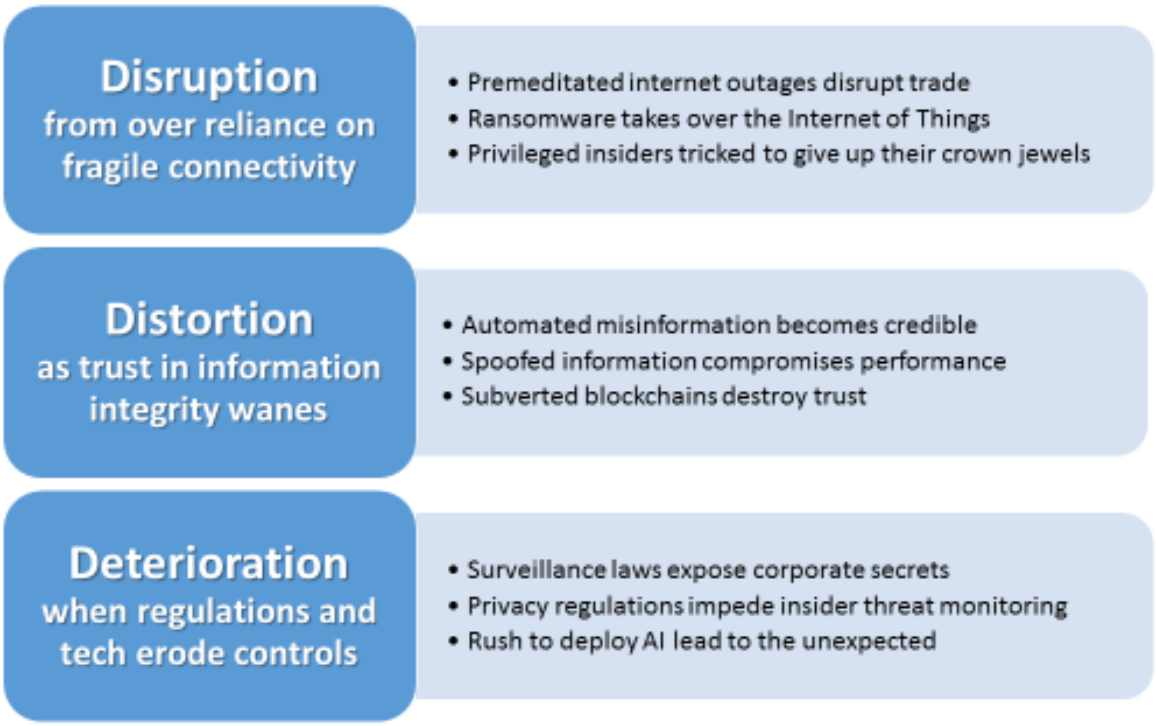

Figure 3. Anticipated threat themes: Information Security Forum cybersecurity threat themes for 2019.

Today, a growing number of organizations view threat landscapes in a more general way, in an attempt to predict the areas of focus for threats rather than specific threats and their precise or relative impacts. In part, this is due to the complexity of today's computing environment. But, in addition, the emphasis on the big picture is driven by the realization that it embeds the foundation, from which the details could be captured and addressed. Figure 3 illustrates this approach and shows a summary of the 2019 threat landscape released by the Information Security Forum (ISF).[7]

The need for generalization is obvious in both cybersecurity threat and technology forecasting. Analysis through knowledge representation provides an opportunity to examine not only the components of the big pictures, but also the connections both between them and within the broader context of deployment or use.

3. Knowledge representation and technology trend prediction

In multi-disciplinary subjects like cybersecurity, knowledge representation approaches could be useful in assessing current and emerging technology spaces, for both research and technology deployment. Ontology-based reasoning can help us obtain a multi-dimensional view of the subject, incorporate consistent constraints, understand dependencies, and draw informed conclusions.

How can we make sense of cybersecurity in a way that can enable multiple and potentially contrasting contexts, including the legitimate use of technology on the one hand, and cybercrime on the other? At a high level of abstraction, the idea is to create a landscape of existing technologies, using their distinguishing features to locate them as points in a multi-dimensional space of concepts. Current trends can then be identified by studying the relative density of points in this space. Higher-density areas denote technologies that are heavily

investigated, or where investment is stronger, while lower-density areas correspond to technologies that have received less interest. Extrapolations can be carried out to determine future trends – possibly by studying how density has changed over a period of time.

But how can we concretely lay out these multi-dimensional points in such a concept space? Essential for a successful exploration of a complex landscape is the ability to link concepts based on their similarity and dependencies, so that more strongly related technologies are closer to each other in the space and can be considered part of a single set from a high-level view.

With ontologies and ontology-based reasoning, it is possible to capture the arbitrary relationships among concepts and most notably class-subclass relationships. An ontology-based approach could permit researchers and practitioners to link together disparate content that draws from similar premises (Iannacone et al. 2015), allowing technologists to reuse, share, and propagate knowledge. We think this approach, which offers mature reasoning capabilities, can be used very effectively to make more informed technology predictions.

3.1 Primary assessment of disruptive technologies

Let us now consider the disruptive potential of distributed ledger technology from a cybersecurity perspective.

Technology foresight and assessment can help to better understand the opportunities and risks for cybersecurity in blockchain by highlighting complex dependencies and risks that are difficult to notice without an ontology. We will illustrate this for the use of blockhain in Internet of Things (IoT) and supply chains. Below are some possible future scenarios to consider that can be developed to first approach the problem: these scenarios (S) are constructed for illustration, and based on assumptions informed by past behaviour.

S1: All key workflows of supply chains including their CIA (Confidentiality, Integrity, Availability) cybersecurity properties, the making of payments, KYM (Known Your Machine) and GRC (Governance, Risk, and Compliance) are mediated through blockchain technology based on open systems.

S2: Many workflows of supply chains, such as the making of payments, are mediated through open blockchains. Some other workflow aspects, such as GRC, cybersecurity, and IoT-facilitated cyber insurance, will be mediated through blockchains ,in which nodes that elect the next block in the chain are controlled by stakeholders in these supply chains.

S3: The paradigm of open blockchains, in which everyone is free to join the network, is not adopted by industries to support aspects of workflows for their supply chains. But blockchain technology is fruitfully and judiciously used to make supply chains more flexible, auditable, secure, and cost effective.

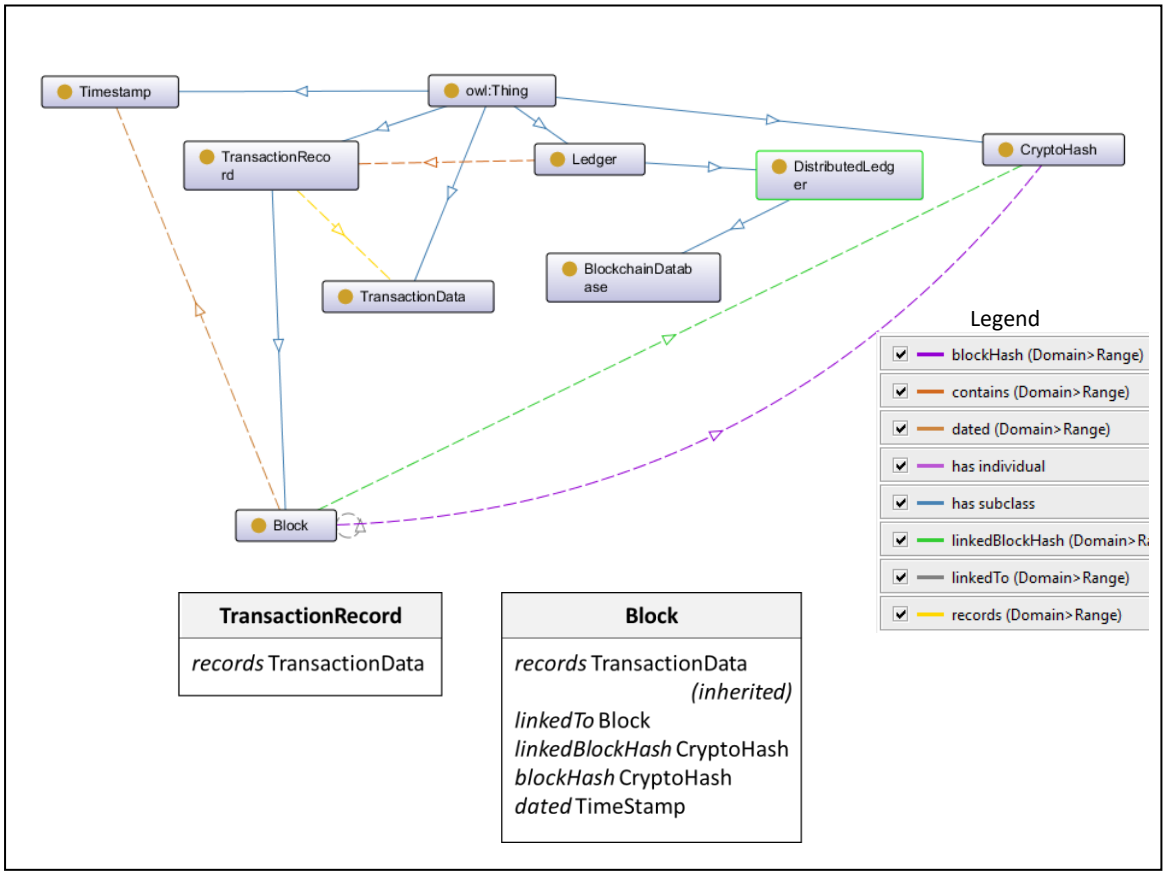

Figure 4. Leveraging Ontologies: A simplified representation of ledgers and blockchains, as they may be used in the process of analysing the three sample scenarios

What is the perceived likelihood of these scenarios and what might be the cybersecurity ramifications of their realization based on the analysis of past behaviour?

Scenario S1 is unlikely because of risks associated with open blockchains: their currencies may not be valid, their governance models may not align with GRC requirements, and open blockchains may not be scalable enough. Confidentiality is a potential issue because transactions and their history would be public, enabling de-anonymization of transactors (Meiklejohn *et al.* 2016).

Scenario S2 appears more likely to us. It is prudent to confine higher-risk aspects to blockchains that have access control (including control of the construction of the blocks) and confidentiality designed into them. And there are cybersecurity concerns about using open blockchains to create and maintain currencies. Smart payment contracts, a key innovation of blockchain, require complex run-time systems that are subject to conventional cyberattacks: the denial of service attack on Ethereum in 2016 (Siegel 2016) illustrates the risks of using a cryptocurrency with limited level of assurance.

Scenario S3 is also likely: developers of cryptocurrencies such as Ethereum are interested in better control of blockchains, through a combination of private and open approaches, to reduce the risks of cyberattacks. Cybersecurity may also be enhanced through advances in privacy-

preserving distributed storage, cryptographic support, more advanced protocols, and other technologies.

Figure 4 above illustrates a simplified ontology as it might be used in the analysis of the scenarios. One of its top-level concepts is “Ledger”, which is refined into “DistributedLedger” and in its subclass “BlockchainDatabase”. A ledger “contains” one or more “TransactionRecord” items, each “recording” a set of “TransactionData”. “Block” is a subclass of “TransactionRecord”, and, as such, inherits relation “records”. It also extends its super-class by relations specific to the workings of blockchains, i.e. “linkedTo” and “linkedBlockHash”, which point to the previous block and store its hash, “blockHash”, which records the hash of the current block, and “dated”, which stores its timestamp. The hierarchical structure of the ontology enables both a high level of abstraction, e.g. viewing blockchain databases as any other ledger, and considering high-granularity details, e.g. using ontology-based reasoning to extract a blockchain from a database by leveraging the “linkedTo” relation. It would not be difficult to extend the ontology further by adding a representation of access control and trustworthiness elements in blockchains, as well as additional dimensions to cover privacy, anonymity, threat agents, and cybercrime.

3.2 From likely scenario to an ontology

Similar scenarios are frequently developed to understand the elements of a field or a use case. How can ontologies help here? As shown in Figure 4, an ontology is a hierarchical specification of classes of objects from a domain of interest, including their properties and relationships. As such, ontologies enable a principled organization of knowledge.

The general-purpose, hierarchical nature of ontologies, their broad applicability, and the fact that all relevant information has an explicit, machine-accessible representation, make ontologies well suited for formalizing multidisciplinary concerns, such as the connection between disruptive technologies, regulatory frameworks, and cybercrime.

When tackling multidisciplinary knowledge, it is useful to divide the formalization into upper ontology and (multiple) domain ontologies. An upper ontology encodes concepts that are common across all domains of interest. For securing cyber-physical systems, for instance, an upper ontology might define the high-level concept of “system component,” with its refinements of “computational device” and “physical device,” and the concept of “vulnerability.” Additionally, a relation “vulnerable-to” might be used to associate a system component with its known vulnerabilities. A high-level concept “activity” can be defined as a super-class of concepts such as “offence,” “analysis,” and “defence” to map out a research taxonomy. In turn, “defence” might be a super-class of “prevention,” “detection,” and “mitigation.”

A domain ontology formalizes a specific knowledge domain. Concepts captured by a domain ontology are specializations of concepts from the upper ontology. For example, a domain ontology of smart grids might describe SCADA systems as kinds of computational devices, power generators as types of physical devices, and list a number of vulnerabilities specific to the smart grid. Relation “vulnerable-to” could then be used to indicate the specific vulnerabilities of smart grid components and types of cybercrime.

Inference can then be applied to propagate relevant properties and relations throughout the ontology. For example, if a new vulnerability is discovered that affects certain system components, one can determine which components are directly vulnerable. A notion of a

component being “affected by” the vulnerability, either directly or indirectly (connected to some other component that is affected by it) can then be analysed through inference to identify, across the ontology, any component that is affected by a vulnerability. This approach may be used in different contexts, to study different dependencies and relations, e.g., between regulatory changes and cybercrime, or technology deployment and cybercrime.

This representation and reasoning framework is especially suited for situations in which knowledge from multiple fields must be captured at the same time. The aforementioned ontology would allow one to study exploits that may affect both the power system and the braking system in a connected vehicle, and also illustrate how cybercriminals might use this vulnerability. Multidisciplinary knowledge can be incrementally and seamlessly integrated, and sophisticated questions about the modelled systems can be answered by means of general-purpose inference mechanisms without the need to develop dedicated algorithms.

Knowledge representation permits us to capture relationships, constraints, and dependencies – important not only in forecasting future trends, but also in obtaining insights about completely different environmental contexts, such as digital business and cybercrime. As an example of this, consider the notion of value chain, a sequence of activities that are performed to produce a product or service and bring it to the market. The general concept of value chain can be easily captured by an ontology, in which activities are linked, by a relation “depends-on”, to the activities they depend on. In a business context, a value-chain ontology can enable the identification of bottlenecks and the evaluation of the effects of new suppliers. However, this ontology can also be applied to studying illegal activities. Kraemer-Mbula (*et al.* 2013) observed the existence of a cybercrime value-chain vulnerability *detection → infection and distribution → exploitation*: by applying the value-chain ontology to illegal activities, dependencies among the various illegal activities can be studied, leading to insights into critical links in the chain and methods for blocking them.

It is worth stressing that all of this is made possible by the semantic nature of the approach. Having precisely defined semantics allows associating ontological languages with inference mechanisms that perform automated, provably correct reasoning. These inference mechanisms enable, for instance, expanding a class-subclass relationship into an ancestor/descendant one. In the value-chain example, the inference mechanisms’ ability to propagate dependencies through a value chain is the key to identifying bottlenecks and critical illegal activities.

4. From knowledge models to risk models

A comprehensive understanding of cybersecurity requirements brought forward by disruptive technologies is not an end goal. Anticipating and producing mitigation in novel environments and for novel uses of technologies is more important. Risk-based methodologies are helpful here.

4.1 Risk Engineering

Traditionally, risk assessments are done for specific, isolated aspects of an environment. Sometimes these aspects are very narrow, such as the functionality of a system component for a strictly defined use case or a reputational risk from a premature release of a potentially disruptive computing device. At other times, these assessments are broader, examining the risks from different threat agents or from actions by people, and the effects of poor processes and new technologies on government systems, examined along these three separate axes: people, processes, and technologies.

The management of multi-domain risks reflecting the complexity of the computing environment can be improved if ICT systems themselves are engineered by explicitly reflecting risks of their use, be it in isolation or in a specific operational context. This approach requires that systems have specifications that articulate risks – be they informal, semi-formal or formal, qualitative or quantitative, given in textual form or within a mathematical model. The body of knowledge associated with various aspects of cybersecurity comprises ways of expressing such risk specifications and analysing the consequences of changing the risk picture. This technique can be also applied to cybercrime.

There is relatively little work on making such specifications composable to scale, and on specifying risks that stem from the combination or interaction of different aspects of systems, such as safety and security. This is where risk engineering can help. Risk engineering can be defined as "incorporation of integrated risk analysis into system design and engineering processes" (Huth *et al*. 2016).

Although full definitions of risk engineering methodologies are wanted, it is clear that they must support an integrated picture of risks, including, at least, the domains of security, privacy, safety, reliability, and resilience (NIST 2017). Success in this area requires several obstacles to be overcome. As mentioned earlier, one challenge is the creation of a comprehensive semantic framework to enable a consistent terminology and ability to reason about the environment based on shared views. A multi-domain ontology can accommodate this requirement. To illustrate this need, even elementary terms, such as "incident," have different definitions within different risk communities: for safety, "incident" denotes an event that does not have safety-critical consequences, whereas for security, it refers to a serious breach.

Another obstacle is lack of a consistent approach to metrics that objectively assess risk and impact, a serious problem when an integrated risk model is considered. To illustrate, failure probabilities in the risk domain of safety are extremely small. But probabilities of a breach in security and privacy, where diverse and evolving attacks must be taken into consideration, are much larger. Thus, successful risk engineering requires integrated, multi-scale risk metrics.

Yet another challenge is risk composition, the ability to measure integrated risks that meaningfully compose risk parameters in multiple domains.

As mentioned in Section 2.5, risk engineering techniques offer advantages for several types of analysis, but especially when applied to an environment experiencing incremental changes, gradually leading to escalation of initially moderate risks. Risk engineering permits us to model and anticipate necessary mitigations for several connected risk domains. To invoke our blockchain example once again, risk engineering helps evaluate, in an integrated fashion, safety, security, and privacy risks introduced by the use of blockchain techniques in autonomous vehicles employing blockchain as a mechanism to support operational data integrity. Subject risks could also include analysis of risks from cybercriminal activity.

Examining cybercrime in isolation from the legitimate use of similar technologies during their lifecycle is not likely to be constructive. Only when cybercrime and technology in general are evaluated based on the same models, including risk models, can we devise a forward looking rather than reactive approach to cybersecurity and cybercrime.

4.2 Cybersecurity Metrics

One of the most serious challenges in cybersecurity is the development of consistent and actionable metrics that could provide insights useful in many areas, such as trends in cybercrime or technology development. Performance management professionals live by the maxim "*measure what matters*." From this viewpoint, the purpose of metrics is to *provide actionable insights to decision makers.* This maxim is valid for technical and socio-technical systems. Cybersecurity metrics must, therefore, be guided by knowledge of what cybersecurity-related insights decision makers' need, both on the security of systems they design or deploy and on the protection of these systems from cybercrime. These metrics will be constrained by the availability (at supportable cost) of suitable data or reliable proxies, and by the timeliness and ease of use of the assembled information.

Understanding impacts is important for creating meaningful metrics based on the cost-effectiveness of investments and operations, safety of persons and assets, legal liability, and similar characteristics. A recent report (Kelley *et al*. 2016) cited "reducing average incident response and resolution times" as the primary cybersecurity challenge of the executives surveyed. As a practical matter, metrics capable of enabling reliable estimation of direct and indirect impacts of system compromise will be essential to informed decision making.

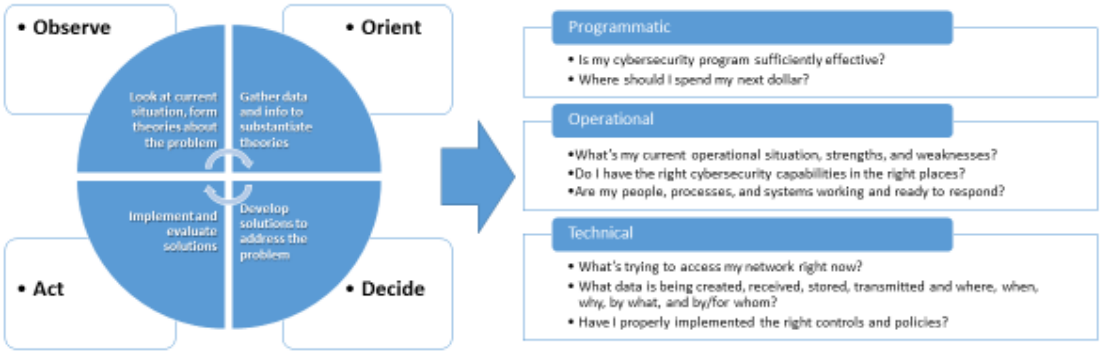

Figure 5. Cybersecurity Metrics and the OODA Loop: Effective cybersecurity metrics ensure decision makers have a fast, reliable OODA loop at multiple levels.

Perfect cybersecurity capabilities would obviate the need for responses by enabling decision makers to prevent incidents. But, as Figure 5 illustrates, decision makers prefer capabilities that enable them to "observe, orient, decide and act" before their adversaries are able to complete the same cycle. While effective cyber reconnaissance and attack campaigns can take months or years to come to fruition, the fact that cyber capabilities operate at machine speed materially affects both the practical usefulness of metrics and the value of research to create them.

In recent years, cybersecurity research and development activity has progressed from an emphasis on *reactive cybersecurity*, which seeks to create and improve tools and processes that can help analysts detect, respond to, mitigate and recover from cyber threats, toward *proactive cybersecurity.* Proactive cybersecurity focuses on creating a "science of cybersecurity" that enables the stakeholders to predict and, ideally, prevent cyber incidents before they happen, and understand when previously compromised nodes will once again become secure.

Reactive cybersecurity capabilities typically centre on detecting anomalies in a system's contents, environment or behaviour. Unfortunately, those who rely on reactive cybersecurity frequently find themselves at a disadvantage, as their strategies and tactics are constantly

disrupted by threat actors finding innovative ways to discover, create, and exploit vulnerabilities.

Proactive cybersecurity draws from metrics-based concepts such as "Cybersecurity Dynamics" developed by Shouhuai Xu and colleagues[8] and relies on "risk-based security metrics" (Thuraisingham *et al*. 2016) that can evolve with the changing environment and proactively account for attack-countermeasure-response dependencies. Recent reports (NIST SPs 800-30, 800-37, 800-39, 800-53, and 800-53A) developed additional dimensions for risk-based and other types of cybersecurity metrics and guidelines (Ross, Feldman and Witte 2016, 5).

Decision makers must know *in advance* whether devices attempting to connect with their networks are sufficiently trustworthy. "[M]easures of trustworthiness are meaningful only to the extent that (a) the requirements are sufficiently complete and well defined, and (b) can be accurately evaluated" (Neumann 2004, viii; Ross, McEvilley and Oren 2016, 1). When coupled with cyber hygiene efforts, reliable metrics of the trustworthiness of a device or environment would offer significant benefits, including protection against cybercrime. Metrics enabling prediction of future failures as a result of attacks are highly valuable, as would be the ability to account for the uncertainty caused by gaps in available data (Newmeyer 2015).

Many efforts noted above recognize that systems designed for reactive cybersecurity make inherent assumptions that may misinterpret or miss useful signals due to interpretational bias. Data-driven AI could also suffer biases as a result of the specific learning processes employed, but adversarial machine learning techniques (Huang *et al.* 2011) may help mitigate this.

How can this concrete wisdom from practitioners be applied to improving the quality of predictions for cybersecurity and cybercrime trends in future technology environments? The challenge lies in adapting the operational signals and related metrics traditionally used in cybersecurity to the techniques for disruptive technology forecasting outlined in Section 2. Optimized cybersecurity metrics for current systems allow us to quantify some parameters of predictive models for disruptive technology, understand the meaning of environmental signals, and improve the building blocks for the ontology supporting more reliable forecasting. Further, such metrics could help improve methodologies for integrated risk engineering and, therefore, contribute to better cybersecurity and improved protections against cybercrime.

5. Conclusions

In "*Principled Assuredly Trustworthy Composable Architectures,"*[9] Peter Neumann states:

> ***[T]here are no easy answers*** *… [C]omplexity must be addressed through architectures that are composed of well-understood components whose interactions are well understood, and also through compositions that demonstrably do not compromise trustworthiness in the presence of certain untrustworthy components."*

In an ideal system, trustworthiness results from the intrinsic logic of the system understood by all its stakeholders. For cybersecurity, this state may never be achievable. But in order to protect our digital infrastructures and combat cybercrime, we need to be ahead of attackers, understand the current state of the ecosystem and its evolution, and comprehend trends in disruptive information technologies, to enable us to anticipate and mitigate cybercrime.

In this chapter, we provided some recipes, techniques, methodologies, and examples that can help technologists and regulators more reliably anticipate the technology trends and develop necessary cybersecurity protections. Most important is to develop cybersecurity models that are broadly applicable and usable for full technology lifecycles and varied use cases as well as for the analysis of cybercrime. Today, use fragmentation in this area makes consistent analysis and reliable forecasts impossible.

Among the tools that can help us make sense of disruptive technologies and render insights to combat cybercrime, several directions of analysis, evaluated in this chapter, appear to be productive. Broader methodological approaches, such as reliance on knowledge representation, development of risk engineering, and creation of objective metrics should be key areas of focus in the multi-disciplinary technology community.

NOTES

[1] See, e.g. "Report on Implementing Federal Cybersecurity Research and Development Strategy," https://www.nitrd.gov/PUBS/ImplFedCybersecurityRDStrategy-June2014.pdf

[2] According to Wikipedia ( )," In computer science and information science, an **ontology** is a formal naming and definition of the types, properties, and interrelationships of the entities that really or fundamentally exist for a particular domain of discourse. It is thus a practical application of philosophical ontology, with a taxonomy. An ontology compartmentalizes the variables needed for some set of computations and establishes the relationships between them."

[3] According to Wikipedia, **Knowledge engineering** (**KE**) refers to all technical, scientific and social aspects involved in building, maintaining and using knowledge-based systems. See https://en.wikipedia.org/wiki/Knowledge_engineering

[4] See, e.g., http://www.eugdpr.org/

[5] See Article 29 Working Party Opinion adopted on 10 April 2014 at https://cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf

[6] The Artcile 29 Working Party Opinion 5/2014 on Anonymization Techniques adopted April 10 2014, p. 6 (https://cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf) describes the reasonableness test as follows: It should be recalled here that anonymisation is also defined in international standards such as the ISO 29100 one – being the "Process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party" (ISO 29100:2011). Irreversibility of the alteration undergone by personal data to enable direct or indirect identification is the key also for ISO. From this standpoint, there is considerable convergence with the principles and concepts underlying the 95/46 Directive. This also applies to the definitions to be found in some national laws (for instance, in Italy, Germany and Slovenia), where the focus is on non-identifiability and reference is made to the "disproportionate effort" to re-identify (D, SI). However, the French Data Protection Law provides that data remains personal data even if it is extremely hard and unlikely to re-identify the data subject – that is to say, there is no provision referring to the "reasonableness" test.

[7] See: https://media.scmagazine.com/documents/217/isf_threat_horizon_2018_execut_54175.pdf

[8] See http://www.cs.utsa.edu/~shxu/socs/

[9] Neumann, P. G. 2004. "Principled Assuredly Trustworthy Composable Architectures," a contract final report presented to DARPA: http://www.csl.sri.com/users/neumann/chats4.pdf, p.151.

References

Bernstein, D. J. 2009. 'Introduction to post-quantum computing,' *Post-Quantum Computing*, Benstein, D. J., Buchanan, J. and Dahmen, E. (Eds.), Heidelberg: Spring-Verlag, 1-14.

Govindarajan, V. and Kopalle, P. K. 2006. 'The Usefulness of Measuring Disruptiveness of Innovations Ex Post in Making Ex Ante Predictions',. *Journal of Product Innovation Management*, 23: 12–18.

Huang, L., Jospeh, A. D., Nelson, B., Rubinstein, B. I. P., and Taylor, J. D. 2011. 'Adversarial Machine Learning', *Proceedings of 4th ACM Workshop on Artificial Intelligence and Security*, ACM, 43-58.

Huth, M., Vishik, C. and Masucci, R. 2016. 'From Risk Management to Risk Engineering: Challenges in Future ICT Systems.' *Handbook of System Safety and Security: Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems*, Griffor, E. (Ed.), , Cambridge, MA, Elsevier: 131-175.

Iannacone, M., Bohn, S, Nakamura, G., Gerth, J., Huffer, K., Bridges, R., Ferragut, E., and Goodall, J. 2015. 'Developing an Ontology for Cyber Security Knowledge Graphs,' *Proceedings of the 10th Annual Cyber and Information Security Research Conference (CISR '15)*. New York: ACM. 1-4.

Kelley, D., Dheap, V., Jarvis, D. and Nordman, C. 2016. *Cybersecurity in the cognitive era: Priming your digital immune system*. Somers, NY: IBM Institute for Business Value, 2016.

Kraemer-Mbula, E. Tang, P. and Rush, H. 2013. 'The cybercrime ecosystem: Online innovation in the shadows?' *Technological Forecasting and Social Change* 80.3 (2013): 541-555.

Kuhlmann, S., Boekholt, P., Guy, K. Heraud, J.-A., Lemola, P., Loveridge D., Luukkonen, T., Polt, W., Rip, A., Sanz-Menendez, L., Smiths, R. and Georghiou, L.G. 1999. 'Improving Distributed Intelligence in Complex Innovation Systems'. Final Report of the Advanced Science and Technology Policy Planning Network (ASTPP), Fraunhofer Institute Systems and Innovation Research.

Meiklejohn, S. Pomarole, M. Jordan, G., Levchenko, K., McCoy, D. Voelker, G.M., and Savage, S. 2016. 'A fistful of Bitcoins: characterizing payments among men with no names.' *Communications of the ACM*, 59(4): 86-93.

Nakamoto, S. 2008. 'Bitcoin: A Peer-to-Peer Electronic Cash System.' https://bitcoin.org/bitcoin.pdf, accessed 20 September 2017.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. 2016. *Bitcoin and Cryptotechnologies: A Comprehensive Introduction*. Princeton University Press, 2016.

NASA 2017. 'NASA Aeronautics Strategic Implementation Plan 2017 Update', NASA Aeronautics Research Mission Directorate.

Neumann, P. G., 2004. 'Principled Assuredly Trustworthy Composable Architectures', Final Report to DARPA, Menlo Park, CA: SRI International,

Newmeyer, N., 2015. 'Changing the Future of Cyber-Situational Awareness,' *Journal of Information Warfare*, 14 (2): 32-41.

NIC 2016. 'The impact of technological change on future infrastructure supply and demand'. UK National Infrastructure Commission report. UK Government.

NIST 2017. *NIST Special Publication 1500-201, Framework for Cyber-Physical Systems: Volume 1, Overview*, Gaithersburg, MD: National Institutes of Standards and Technology.

Quinn, J.B., 1967. 'Technological forecasting.' *Harvard Business Review* 45(2): 89-106.

Rao, G.A. and Mahulikar, S.P. 2002. 'Integrated review of stealth technology and its role in airpower', *Aeronautical Journal* 106(1066): 629 – 641.

Ross, R., Feldman, L. and Witte. G. (eds.). 2016. 'Rethinking Security through System Security Engineering', ITL Bulletin for December 2016, NIST Information Technology Laboratory, accessed 21 December 2016 at http://csrc.nist.gov/publications/nistbul/itlbul2016_12.pdf.

Ross, R. McEvilley, M., and Oren. J. C. 2016. *NIST Special Publication 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, Gaithersburg, MD: National Institutes of Standards and Technology.

Shor, P.W. 1995. 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer', *SIAM Journal on Computing*, 26(5): 1484-1509.

Siegel, D. 2016. 'Understanding the DAO Attack', Coin Desk, 25 June 2016, accessed on 20 September 2017 at https://www.coindesk.com/understanding-dao-hack-journalists/.

Thuraisingham, B., Kantarcioglu, M., Hamlen, K., Khan. L., Finin, T., Joshi, A., Oates, T. and Bertino, E. 2016. 'A Data Driven Approach for the Science of Cyber Security: Challenges and Directions', *Proceedings of the IEEE 17th International Conference on Information Reuse and Integration*, Piscatawy, NJ: IEEE, 1-10.

Van Zwanenberg, P., Ely, A. and Stirling, A. 2009. 'Emerging Technologies and Opportunities for International Science and Technology Foresight', STEPS Working Paper 30, Brighton: STEPS Centre.