serene risc Digest Winter • 2014

Cutting Edge Research Summaries for Policy-Makers and Practitioners

What is the real impact on market value of cyber attack announcements?

This research uses market value, as an indicator of shareholder confidence, to examine the potential risk from breaches of information security. A cybersecurity breach is anticipated to have an economic cost evidenced by a change in stock price. This hypothesis is tested using reports of 128 cyber attacks on 81 firms, from a wide range of industries. For each of the 128 attacks, the cumulative abnormal return is calculated over several different time periods, to quantify how news of a cyber attack might create an unpredicted stock value return. The results demonstrate an overall negative stock market reaction to public announcements of information security breaches. For firms in the financial sector, the impact is not always negative, especially in shorter time frames.

Do privacy violations and security breaches affect banking behaviour?

All companies are vulnerable to cyber threats. Not all incidents are identical and the nature of a breach may influence how people react. This study uses an experimental method to examine the economic impact of privacy violations and security breaches on trust and behaviour. All participants were presented with a fictional bank scenario. In some of the descriptions there was no data protection problem, but in others the bank experienced a privacy incident or a security incident. After reading about the bank, each participant was given 10 Euro, of which they could invest some, all or none in a financial product of the bank. The largest average investments came from the group shown no data protection problem. The group exposed to the security breach made the lowest investments. This research reinforces the imperative for security by quantifying the potential monetary loss of security breaches and privacy violations, a method which could be useful for cost-benefit analysis of security interventions.

Are users on board with information security practices?

Measuring user satisfaction is one way to evaluate whether people are following information security practices, and why. Understanding what features improve user satisfaction might also inform the design of systems that are both functional and accessible. Users understand that there is some benefit from information system security. Complex information security practices are seen as barriers and are related to lower user satisfaction. Several features of information systems - such as information and system quality - are related to higher user satisfaction. Dissatisfied users can be a risk for protection, so ensuring user satisfaction is an important part of designing a successful information security system.

What password policies and practices actually improve web security?

A traditional approach to web security focuses on user password choices. Adding strength and complexity to the character combination used in passwords is only one way of enhancing security. While adding uppercase and special characters does marginally improve resistance, not enough that 'stronger' passwords are themselves an effective strategy for web security. Several methods can improve resistance to attack more effectively; for example, password 'blacklists' that prohibit commonly used choices can be built from leaked lists. Other methods also rest within the control of the site administrator. Key steps in protecting passwords from breach include using non-plaintext storage and one-way encryption. To promptly detect leaks, the password file can be spiked with false passwords that signal an attempted attack and the system can lock out users for too many unsuccessful attempts at log in. Site administrators' can take responsibility for a greater share of password security.

What does the public view as a serious cybercrime ?

Public views inform what acts are considered to be crimes and how those crimes are punished. What types of crime does the public define as serious? This study is informed by online surveys completed by participants who read a description of a fictional cybercrime scenario. In each case, the situation involved the intentional breach of consumer personal information. Experiments slightly varied the causes and consequences of the breach in different scenarios – e.g. amount or sensitivity of breached data, motivation of the attacker, and consequences of the breach. People distinguish between features of cybercrimes. The amount of data stolen and motivation of the attacker held significant weight in the perception of seriousness. The seriousness was perceived as greater if more data was breached or the intention was profit-making. Individual attitudes towards privacy, including experiences of identity theft and data protection, are related to views on seriousness of crimes. In responding to a cybercrime, firms can strategically use information about the event recognising that details about a breach can impact the public perception of a crime.

What works to train cybersecurity experts?

Formal education and informal training are both understood to contribute to the making of cybersecurity professionals for various capacities. This study examines how current cybersecurity professionals got where they are. The factors considered include the time spent in various types of training and self-reported current level of expertise. On average, the cybersecurity professionals in the study had more years of informal training than formal education. Practical experience and on-the-job training are valued highly for building expertise – in terms of both the level and breadth of skill obtained. The perspectives of cybersecurity professionals on their formative influences could shape training to integrate the benefits of both structured and experiential learning.

What are young adults thinking when they share 'those photos'?

For some, the widespread use of social media and communication technologies has brought an acceptance of the decline of privacy. The technological ease of sharing information is prompting a renegotiation of 'reasonable' expectations of privacy. This study explores young adults' expectations of privacy surrounding the practice of sexting. Participants were presented with two scenarios that involved sexting. They were then asked what privacy might reasonably be anticipated by the person who shared the sexual content, as well as asked whether they themselves would further distribute the material. People expect a high degree of privacy, with the majority of respondents indicated it is **rarely** or **never** okay for someone to share a sext further without permission of the original sender.

Why do people cooperate with scams?

Scams are a variety of fraudulent activity that requires victims' willing cooperation. Modic and Lea develop a model of susceptibility, which is used to determine the influences that are strongest in getting people to comply with scams. This approach considers various levels of compliance. Individuals were asked if they had ever been victim of fraud and, if so, what influenced their compliance. More than half of respondents found scams plausible, which is the first step in their willingness to comply. Once people have shared information, they are more likely to also give money. These findings point to a progression in the compliance with scams, from seemingly innocuous engagement to forms of participation that present greater risks. Respondents who indicated a high need for consistency were more likely to give information and those with low self-control are more likely to give money. The factors that influence susceptibility could be considered in fraud prevention and awareness campaigns.

Using friendlies as shields. How can cyber missions reduce the risks of cyber friendly fire?

One of the outcomes of ineffective information flow in military organisational structures can be accidental material harm to an ally. Cyber fratricide is the unintentional interference between operational or tactical elements of friendly forces and causing harm. In cyber exchanges connections created for observation and action in cyberspace may allow an adversary observation and action back into the instigating organisation. The current method of mapping areas of operation for cyber engagement is underdeveloped. There are other strategies for minimising the risk of cyber fratricide, including creating feedback loops in operational planning phases to improve agility of situational awareness in particular. Redefining duties of established positions would also improve accuracy in the cyber realm and could thereby reduce the risk of cyber fratricide.

How can cyberspace be framed for operational military activity?

Armed forces in Canada are organized around the environment in which they operate. Like land, air, and sea, cyberspace can be a source of threats. Actions initiated in the cyber realm can impact other domains. However, despite the similarities, cyberspace challenges traditional military conceptions of environment because as an environment it is impermanent and malleable. Cyberspace may not constitute a domain separate from air, land, and sea. Cyberspace might instead be understood as a supporting or enabling function for military capabilities on land, on sea, and in the air, more akin to a special operations role than a domain unto itself. As the understanding of and experience with warfare in cyber space evolves, so too might the definition of domains.

What will cyber resilience mean in the future?

Cybersecurity is of high strategic importance but perhaps the landscape has not been laid properly to ensure resilience. Systems for the governance of cyber-defence are inadequate, with many of the functions that contribute to resilience under private ownership. Governments are, at once, trying to increase secrecy while also encouraging cooperation and accountability. The government itself has limited in-house expertise. In effect, the operational capacity for surveillance and cyber-defence action rests in the telecommunications industry. In this context, governments can leverage other actors who hold the operational capacity to promote and increase resilience. Solid defence also includes systems diversity, that is a mix of analog or manual checks and balances in addition to digital safeguards.

The Effect of Information Security Breaches on Stock Returns: Is the Cyber crime a Threat to Firms?

As firms are increasingly connected through information technologies, information security is of greater concern. Information security measures of protecting the accessibility, integrity and confidentiality of information must also include avoiding the costs of breaches – both in remediating any infrastructure damage and repairing reputation. This important concern competes with other organizational financial and operational priorities. This research uses market value, as an indicator of shareholder confidence, to examine the potential risk from information security breaches from cyber attack.

In this study, the authors look for change in the market value of a firm in the days surrounding an announcement of a cyber attack, using an 'event study' methodology. This approach assumes that the market will reflect changes in customer behaviour in response to a particular event, isolated from other factors. A cybersecurity breach is anticipated to have an economic cost evidenced by a change in stock price. This hypothesis is tested using reports of 128 cyber attacks on 81 firms, from a wide range of industries, including soft drink producers, computer and software retailers, aircraft manufacturers, interior design services, and more. Of these, 34 events concerned 17 financial and insurance sector institutions. Information on cyber attacks over the period from 1995 to 2012 was drawn from a database of newspaper reports (Factiva) and stock market price of firms was obtained from the Datastream database. For each of the 128 attacks, the 'cumulative abnormal return' was calculated over several different time periods. Abnormal returns are a measure of how the stock return on the day a cyber attack is announced differs from the predicted or normal stock return. The cumulative abnormal return is the sum of these differences over several days.

The results demonstrate an overall negative stock market reaction to public announcements of information security breaches. The findings are less conclusive when the results are examined separately for firms from different sectors. For firms in the financial sector, the impact is not always negative, especially in shorter time frames. For firms from other sectors, the average impact of announcements about cyber attacks is a negative market return. This confirms the results of other studies showing that, although the impact is often a negative, the effect of cyber attacks is, in fact, variable.

Understanding the impact of a cyber attack on stock market return is key to making well-informed decisions about investments in information security activities. Any risk assessment must consider changes to market value among the impacts of a cyber attack.

A change in stock market return should be included in the risk assessment of cyber security for firms.

Arcuri, M. C., et al. The effect of information security breaches on stock returns: Is the cyber crime a threat to firms? European Financial Management Association 2014 Annual Conference. University of Rome Tor Vergata - School of Economics.

The Economic Impact of Privacy Violations and Security Breaches

All companies are vulnerable to cyber threats. Any attack can have significant consequences, including direct costs incurred in customer support, security improvements, and investigations. Indirect costs might include an erosion of trust in the corporation, and an undermining of potential clients' buying intentions. Not all incidents are identical and the nature of a breach may influence how people react. Privacy, the ability to control the use of one's own personal information, is different to security. The latter is a feature of privacy, also encompassing steps to ensure integrity and confidentiality of personal information. Different responses to privacy violations and security breaches illustrate a range of economic impacts that can stem from data compromise.

This study uses an experimental method to examine the economic impact of privacy violations and security breaches on trust and behaviour. By conducting the experiment in a laboratory, rather than studying a series of real events, researchers were able to better control a range of conditions. Nearly 120 participants were presented with a fictional bank scenario. In the situations described, either 1) no data protection problem occurred, or the bank experienced 2) a privacy incident (i.e. the transfer of client information without customer consent) or 3) a security incident (i.e. theft of customer information by a former employee). After reading about the scenario, each participant was given 10 Euros, and the choice to invest some, all or none in a financial product of the bank. The average proportion of the money invested was then compared between groups.

The largest average investments came from the group shown no data protection problem. The group exposed to the security breach made the lowest investments; this suggests that security breaches may be related to a greater economic impact than privacy violations. In the group aware of the bank's privacy violations, the impact was on trust, not investment behaviour.

This research reinforces the imperative for security, by quantifying the potential monetary loss of security breaches and privacy violations. This could prove useful for cost-benefit analysis of security interventions. Further, it illustrates that there is also an impact of trust that might not correspond directly to investment decisions, but could nonetheless have ramifications for financial institutions' dealings with their clients.

Trust is important to bank clients but they consider privacy and financial security differently which could affect their response to communication of incidents.

Nofer, D.-K. M., et al. "The Economic Impact of Privacy Violations and Security Breaches." Business & Information Systems Engineering: 1-10.

Measuring User Satisfaction with Information Security Practices.

Successful information security depends upon effective technical components, but also on proper interaction with those tools by human users. Measuring user satisfaction is one way to evaluate whether people are following information security practices, and why. Higher levels of user satisfaction are often connected with more effective use of the information systems. Accordingly, understanding what features improve user satisfaction might also inform system designs that are both functional and accessible.

This study surveyed more than 170 corporate information system users in Brazil. To explore individual security behaviours, the survey elaborated on the ideas from several theories of motivation. For information security system practices, this includes features such as usability and perceptions of system performance.

The findings show that people know why information security practices are important. Users understand there is some benefit from information system security. However, users are also wary of potentially complex security controls, which may make it harder for them to get their work done. Complex information security practices are seen as barriers and are related to lower user satisfaction. However, several features of information systems are related to higher user satisfaction:

- Information quality: e.g., reliability and completeness of information
- System quality: e.g., user friendliness and response time
- Support service e.g., quality, promptness and responsiveness
- Work performance: e.g., increased efficiency, and
- Work relationships: e.g., supports the social needs of the user.

Dissatisfied users can be a risk for protection, so ensuring user satisfaction is an important part of designing a successful information security system. Users can be engaged in security by being included in the development of corporate practices and policies, as well as through awareness policies and with engaging training. The survey developed in this study can be used to identify issues with user satisfaction and to formulate policies that align with both user and organisational needs.

Security measures that reduce the capacity of systems to satisfy user expectations are less effective because they can disengage users from security efforts.

Montesdioca, G. P. Z. and A. C. G. Maçada (2015). "Measuring user satisfaction with information security practices." Computers & Security 48.

An Administrators Guide to Internet Password Research

A traditional approach to online account security focuses on user password choices. Adding strength and complexity to the character combination used in passwords is only one way of enhancing security. Users devote an effort to password selection relative to the perceived consequences of compromise. This effort ranges from negligible, as in the case of trivial accounts, through high-consequence accounts requiring hard-to-guess passwords, to ultra-sensitive accounts requiring multiple forms of authentication. Users will budget their effort to match their view of the risk, so will be reluctant to invest time and energy in complex passwords for low-priority accounts.

This article examines what is known to work, or not work, and what is unknown in password policies. One of the tools available for this research are lists leaked from hacked websites. These databases instructively show which passwords are often used, as well as how often. In light of that evidence, Florencio et al. propose that some notions of password strength and complexity are unhelpful. A combination of characters that is objectively strong (e.g. P@ssword$) when evaluated by an algorithm, might still be vulnerable to guessing. Traditional measures of resilience to password guessing attacks assume passwords are selected randomly. However, evidence shows that people tend to reduce the effort required by re-using common passwords. Password complexity rules that overlook these patterns of use are ineffective at improving password resilience. As a result, complex but commonly used passwords could still be easily guessed. Adding character types marginally improves resistance, but not enough that 'stronger' passwords alone are an effective strategy for web security.

There are several types of attack to consider when evaluating password resistance (see table below). An online attack occurs at the public-facing website, when an attacker guesses the correct username and password combination and the server grants access. These attacks can be automated but may be carried out simply with only a browser and web access. An offline attack occurs when an attacker gains access to a stored password file without being detected, and when passwords in the file are one-way encrypted. Some methods to improve resistance to attack are listed in the table below.

Attack		Guesses	Recommended defences
Online guessing	Breadth-first	10^4	•Password blacklist •Rate-limiting •Account lock-out •Recognition of known devices (e.g., by browser cookies, IP address recognition)
	Depth-first	10^6	
Offline guessing	Breadth-first	10^{14}	•Iterated hashing •Prevent leak of hashed-password file •Keyed hash functions with Hardware Security Module support
	Depth-first	10^{20}	
Rainbow table look-up (using extensive pre-computation)		n/a	•Salting •Prevent leak of hashed-password file
Non-guessing (phishing, keylogging, network sniffing)		n/a	•Not a password guessing issue

Although character combination and special characters provide only minimal security, there are more productive options for channeling user choice of password (e.g. password 'blacklists' that prohibit commonly used choices built from leaked lists). By preventing use of these passwords, administrators can premptively deal with the highest risk selections. However, blacklists might annoy some users and are not a permanent fix, as some common passwords change with time.

Other methods also rest within the control of the site administrator. Key steps in protecting password files from breach include using non-plaintext storage and one-way encryption. To promptly detect leaks, the password file can be spiked with false passwords that signal an attack and the system can lock out users for too many unsuccessful attempts at log in.

The evidence supports increasing site administrators' responsibility for password security. Overall, a single approach to all users or all types of accounts may not be the most effective strategy to ensure security. More rigid limits might be readily accepted by users with high-consequence accounts, while the same restrictions might be prohibitive for those with less investment in a particular online account.

Complex passwords are a small part of password security, reasonable passwords with attentive administration can provide greater protection than user responsibility oriented policy.

Florêncio, D., et al. (2014). An Administrator's Guide to Internet Password Research. Proceedings of USENIX LISA, Seattle, WA.

Experimental Measurement of Attitudes Regarding Cybercrime

Public views inform what acts are considered to be crimes and how those crimes are punished. Measuring public perception provides insight beyond assessing impact on victims or the economic cost of crimes and penalties. Gauging perceptions is a delicate task of distinguishing how people understand their world. In the case of perceptions of cybercrime, these attitudes can be hard to define and measure using standard scales. What makes a crime 'serious'? What types of crime does the public define as serious?

This study is informed by online surveys completed by 2440 participants from across the U.S.. Each participant read a description of a fictional cybercrime scenario. In each case, the situation involved the intentional breach of consumer personal information, with slight variations in the causes and consequences of the breach in different scenarios. The study compares how responses might differ according to the characteristics described in the scenario. The features that varied were:

- Type of data stolen - whether name and contact information or medical records;
- Scope - amount of data stolen;
- Motivation of the attack – profiteer, activist, or student;
- Organisational responsibility – the company's diligence and disclosure;
- Consequences – the cost and who paid (i.e. the business or its customers); and
- Context – if the victim firm was a bank, government agency or non-profit.

In completing the surveys, participants rated the seriousness of the crime in terms of harmfulness and wrongfulness (i.e. an evaluation of the moral gravity) and recommended punishments.

The results show people distinguish between features of cybercrimes. People judged an attack as more serious when larger amounts of data were stolen. The motivation of the attacker also held significant weight in the perception of seriousness. If the intention was profit-making, the seriousness was perceived as greater. Also when the cost of consequences was higher or when the data breached more sensitive, such as personal health information, people perceived the attack as more harmful and recommended harsher punishment. Individual attitudes towards privacy, including experiences of identity theft and data protection, are related to views on the seriousness of crimes. Someone more concerned about privacy will tend to rank crimes as more harmful and wrongful, and thus recommend harsher punishment.

Public views suggest serious crime is perceived as acts that are wrongful and harmful, in particular those that have a widespread impact or are motivated by personal profit of the attacker. This suggests the types of crime that might be of greatest concern to consumers – such as those that breach sensitive information and have a high cost of remediation. In responding to a cybercrime, firms can employ breach disclosure strategically recognising that the details of a breach can impact public perception of a crime.

Not all cyber thefts are considered equal. The perceived seriousness of an event depends on value and motivation of the theft but also on the response of the organisation attacked.

Graves, J. T., et al. (2014). Experimental Measurement of Attitudes Regarding Cybercrime. 13th Annual Workshop on the Economics of Information Security. Pennsylvania State University.

Using Cognitive Task Analysis to Investigate the Contribution of Informal Education to Developing Cyber Security Expertise

Although cybersecurity expertise is a highly sought competence, there is no agreed educational path to developing the necessary professional skills. Formal education and informal training are understood to both contribute to the making of cybersecurity professionals for various capacities.

This study examines how current cybersecurity professionals got where they are. An online survey of 131 participants and follow up interviews with 10 professionals asked about such dimensions of their education as the time spent in various types of training and self-reported current level of expertise.

The cybersecurity professionals in the study on average had more years of informal training (self-taught) than formal education. Many perceived their advanced aptitude as being fostered through experiential learning. Education was seen as a convention. Experience was ranked as the key ingredient to becoming an expert, rated more highly than education and pure knowledge. Similarly, on-the-job training was ranked above classroom learning and experimentation as a source of knowledge. Self-reported skill level was shown as being correlated with informal education but not with formal training; those with an expert skill level reported more informal training than those with high or intermediate skill. The results for breadth of skill are similar. Experts reported being skilled in more areas than those with intermediate and even high levels of skill.

This research has implications for the design of training opportunities. Importantly, pursuing formal and informal education should not be presented as an 'either/or' choice. Cybersecurity education programs could make the most of benefits of informal training, by integrating practical and experiential learning.

A combination of formal and informal training incorporating experiential learning is important in creating cybersecurity experts.

Champion, M., et al. (2014). Using Cognitive Task Analysis to Investigate the Contribution of Informal Education to Developing Cyber Security Expertise. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, SAGE Publications.

Sexting in Context – Privacy Norms and Expectations

For some, the widespread use of social media, and information and communication technologies (ICT) has brought an acceptance of the decline of privacy. This perspective is particularly strong in judgments overlooking violations of privacy when the victim has willingly shared sexual content. The technological ease of sharing information is shifting behaviours, especially among youth and young adults whose engagement with and through social media and ICT is pervasive and personal. Where some might suggest the only way to maintain privacy is to not share private information, a new technological context is fostering new expectations.

This article challenges traditional expectations of privacy by exploring the practice of sexting – sending sexually explicit images or messages via the Internet or mobile phones – as a form of consensual communication. Rather than inviting violations, those who sext take care of their reputation and make effort to preserve privacy online.

This study explores the expectations of privacy surrounding the practice of sexting. Through an online survey and focus group, participants were presented with two scenarios that involved sexting. They were then asked what privacy might reasonably be anticipated by the person who shared the sexual content, as well as asked whether they themselves would further distribute the material.

The majority of respondents indicated it is rarely or never okay for someone to share a sext further without the permission of the original sender. The reaction to a privacy violation depends on the nature of the relationship and how the content was shared. When the sender and recipient are dating, expectations of privacy increase with the length of a relationship so that there is a greater expectation of protecting privacy in longer-term relationships. The most acceptable form of sharing was a recipient showing the content on their own phone. Increasingly public methods with greater potential for wider distribution, such as forwarding the message or posting to the web, were indicated by respondents as progressively more inappropriate. All participants expressed high expectations for privacy, with 90% of women and 80% of men indicating sharing was never acceptable.

People want privacy to coexist with the consensual sharing of sexual content. This is the root of context-specific privacy norms, which reveal that although people seek opportunities to share, the expectation of privacy remains. These expectations also shift, and may differ among populations of different ages and different levels of technology integration. Understanding the privacy expectations of a user group is an important tool for understanding the nuance of reasonable expectations of privacy in online communications and meeting their needs as customers. These findings could inform the design of safer sharing technology.

Privacy online is context specific. Sexting is considered to be a private activity. Providing software, systems and policy that support this expectation is important in providing a safe cyberspace.

Hasinoff, A. A. and T. Shepherd (2014). "Sexting in Context: Privacy Norms and Expectations." International Journal of Communication 8: 248.

Scam Compliance and the Psychology of Persuasion

Scams are a variety of fraudulent activity that requires victims' willing cooperation. So why do victims agree to participate, given that doing so will likely be against their own best interests? Various factors have been identified in research on psychology of persuasion, and some are particularly applicable in motivating compliance with scams.

Building on literature about persuasion, Modic and Lea develop a model of susceptibility, which is used to determine the influences that are strongest in getting people to comply with scams. This approach considers various levels of compliance, from an individual finding the fraud to be plausible (and therefore being open to further participation), to sharing personal information, all the way to giving money.

Individuals were presented with various fraud scenarios (such as fake cheques, phishing schemes, and lottery scams), asked if they had ever been victim of one of these types of fraud and, if so, what influenced their compliance. One study inquired about experiences over the participants' lifetime, while another focused on incidents of fraud within the last three years.

Four factors were found to contribute to individual susceptibility:

- Influence of authority (e.g. the degree of trust in authority figures)
- Social influence (e.g. the power of peers)
- Self control (e.g. when low, suggests a lack of filter for impulses)
- Need for consistency (e.g. to seek structure and a desire to honour commitments)

More than half of the respondents found the scams plausible, which is the first step in building their willingness to comply. Once people have shared information, they are more likely to also give money. These findings point to a progression in the compliance with scams, from seemingly innocuous engagement to forms of participation that present greater risks. Respondents who indicated a high need for consistency were more likely to give information and those with low self control were more likely to give money. Student respondents were more likely than non-student respondents to give both information and money, especially in Internet fraud scenarios. Although the study considered demographic factors, the results are inconclusive on the role of age and education level in predicting compliance. For example, younger people appear more sceptical when presented with fraudulent activity, but that suspicion does not necessarily translate to less compliance. In this way, the findings are consistent with the competing results among other studies that consider demographics and compliance.

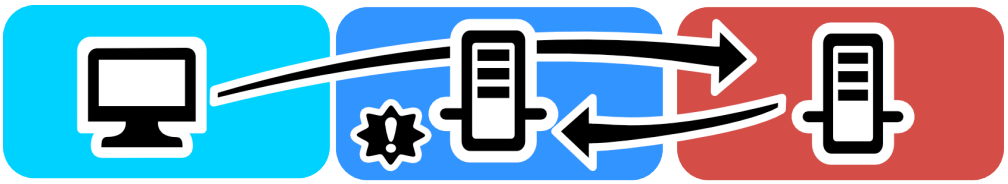
The factors that influence susceptibility could be considered in fraud prevention and awareness campaigns. Fraud prevention activities could expose the key strategies used in scams to motivate people and provide tools for people to use in filtering what they hear and how they respond.

People fall victim to fraud for a variety of reasons. Security measures that consider fraud susceptibility factors could be more effective.

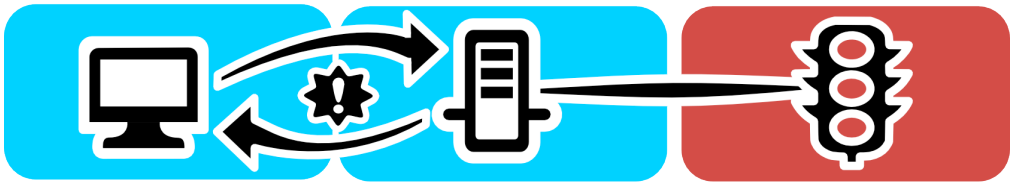
Modic, D., and Lea, S. E. (2013). Scam Compliance and the Psychology of Persuasion. Journal of Applied Social Psychology.

Cyber Fratricide

In the US military, roles are separated by function. Liles and Kambic weigh the impact of this structure for cyber defence. When layered with intentional secrecy of military operations, the result is a breakdown in the flow of information. Silos are not uncommon in communication within organisations, but the stakes are particularly high when the mandate includes offensive and defensive action intended to cause harm. One of the outcomes of this ineffective information flow can be accidental material harm to an ally. Cyber fratricide is the unintentional interference between operational or tactical elements of friendly forces involving the compromise or liquidation of assets, information, or capabilities of those forces.



Operations in the cyber realm may be more vulnerable to this sort of interference. Cyber exchanges are, by nature, transactional, unlike other forms of access or observation. This means that connections created for observation and action in cyberspace may allow an adversary observation and action back into the instigating organisation. So the observer cannot use their own network connections to conduct an attack and must equally be cautious about use of other allied networks.



Routing operations through friendly servers can create conflict between cooperative interests. For example the friendly party (shown in the middle) may identify unauthorised use and deploy countermeasures, or the target (red, on the right) may retaliate or block connections, thus placing friendly parties at risk. Minimal action in any direction can compromise the integrity of the infrastructure. In addition to possibly infecting, attacking, or degrading service to friendly nodes during execution of the attack, an attack may incidentally grant enemy access to the network or destroy friendly assets in the course of defensive duties.

Further complications can also arise. In the hypothetical scenario where a Traffic Management System (TMS) is exploited to create tactical advantage for ground forces, it is very possible that the TMS service administration is outsourced, even to a firm within the friendly territory. Actions to compromise that system could be considered as a war crime as military actions launched against civilian parties. Furthermore any security measures employed by that firm could be considered as acts of treason as they would aid the adversary.

The current method of defining area of operation for cyber is underdeveloped: "Without a mapping function that allows for holistic situational awareness and targeting of cyber assets both physically and logically, the current construct for area of operation is not only incomplete and ineffectual" (p337). Such a mapping function would increase the accuracy of engagement. Creating more assessment and feedback points in operational phases would improve agility and situational awareness particularly when feeding in assessments from prior information operations. Redefining duties of established positions would also improve accuracy in the cyber realm and could thereby reduce the risk of cyber fratricide.

Poor information flows can lead to the degradation or complete failure of an operation possibly at the cost of life or infrastructure. Network compromise or mission failure can also reverberate beyond the operation, affecting the entire organisation. Even when confidentiality is paramount, organisations can consider structural changes that improve sharing of information at critical points and using accurate, holistic mapping of cyber resources.

There is no defined warzone for cyberwar; conflict almost always involves friendlies and non-combatants. Secrecy and poor awareness in cyber operations can place outcomes, allies and citizens at greater risk of harm.

Liles, S. and J. Kambic (2014). Cyber Fratricide. 6th International Conference on Cyber Conflict. P. Brangetto, M. Maybaum and J. Stinissen. Tallinn, Estonia, NATO Cooperative Cyber Defence Centre of Excellence.

On domains: Cyber and the Practice of Warfare

Armed forces in Canada are organised around the environment in which they operate. Cyberspace may not constitute a domain separate from air, land, and sea.

The traditional domains of warfare evolved as technological innovations introduced new ways for people and nations to exert physical force against each other. Each of the three key domains – air, land, and sea – presents unique challenges and opportunities and requires a different approach to military action. Operations on land differ from seaborne or airborne activities. Domains also share common qualities that are key to their classification. Each has a dimensional quality that military forces seek to control, with the goal of establishing freedom of action for friendly forces and denying the same to their adversary. Actions in any one environment might influence another, but in each the goal is to control a portion of that particular domain.

Actions in cyberspace can be a source of threats and can impact on other domains. However, despite the similarities, cyberspace challenges traditional military conceptions of environment because it is impermanent and malleable. A military cannot physically exist there, in the same way that an armed force can occupy a physical environment. The friction is not new. cyber war is an extension of theories and concepts that have historically challenged military doctrine; such as information warfare, command and control warfare, and network-centric warfare, which are not in themselves separate domains.

Reserving the label of a domain for the traditional environments of air, land, and sea reflects the accepted understandings of how to achieve military effects. The authors suggest that, as the understanding of and experience with warfare in cyber space evolves, so too might the definition of domains.

Definitional debates continue about how cyberspace fits into existing understandings of risk and response. While there is agreement that force and influence can be projected through cyberspace and there are some issues in common between addressing threats in physical domains and in cyberspace, the latter is not different enough to constitute a separate domain. Cyberspace might instead be understood as a supporting or enabling function for military capabilities on land, on sea, and in the air, more akin to a special operations role than a domain unto itself.

Military cyber operations support physical operations and separate management is not yet necessary.

McGuffin, C. and P. Mitchell (2014). "On domains: Cyber and the practice of warfare." International Journal: Canada's Journal of Global Policy Analysis.

The Future of Cyber Resilience in an Age of Global Complexity

Cybersecurity is of high strategic importance but perhaps the landscape has not been laid properly to ensure resilience. Systems for governance of cyber-defence are inadequate, with many of the functions that contribute to resilience under private ownership.

An increase in the critical national infrastructure that is privately controlled reinforces the tension between working collaboratively and confidentiality. Governments are, at once, trying to increase secrecy while also encouraging cooperation and accountability. This is paradoxical for many types of relationships - within government, such as between departments or agencies, as well as in public-private partnerships and across state borders. Although often viewed positively, collaboration is related to the diffusion of responsibility for cyber-defence. For example, the European Network and Information Security Agency (ENISA), which encourages convergence and co-ordinates regulation among European states, is one example of a regional alliance for cyber-security.

The government itself has limited in-house expertise. In the case of the United Kingdom, as much as 80% of critical national infrastructure is privately owned. In effect, Herrington and Aldrich argue, the operational capacity for surveillance and cyber-defence action rests in the telecom industry. In encouraging partnership, government has fostered private ownership of resilience. However, should something go wrong, the public will nonetheless look to government; "[t]he public are unlikely to blame the telecoms and specialist Internet providers they have barely heard of, still less fellow citizens with a relaxed approach to anti-virus protection. When the digital tsunami occurs, citizens will hold government to account for the failure of an infrastructure they no longer own or control – and which ministers do not fully understand." (p303)

There is a certain inevitability to further exponential increase in the available data and in integration of technologies providing that data. This 'connectedness' will present greater risks to privacy and security, but also holds the potential for greater transparency; publics can learn more about their government and private industry providers, information which can be used for holding service providers to account. In the face of increased private ownership of resilience, robust security requires legislating duties for service providers. Governments can leverage other actors who hold the operational capacity to promote and increase resilience. Solid defence also includes systems diversity, that is a mix of analog or manual checks and balances in addition to digital safeguards.

Convergence of technology and diffusion of responsibility and expertise creates issues for the resilience of cyberspace. Government may be expected to provide cyber safety regardless of who owns and operates the infrastructure.

Herrington, L. and R. Aldrich (2013). "The Future of Cyber-Resilience in an Age of Global Complexity." Politics 33(4): 299-310.

SERENE-RISC Six Key Activities

Smart Cybersecurity Network (SERENE-RISC) is a knowledge mobilisation network organises six key activities intended to reach its various audiences: workshops and seminars, a knowledge brokers' forum, quarterly knowledge digests, Konnect - online knowledge-sharing platform, a public website and a professional development program.

The latest developments and upcoming activities for each of the six key activities is shown below.

The SERENE-RISC Quarterly Cybersecurity Knowledge Digest

2014 Winter

Editor-in-Chief Michael Joyce; **Editor** Emily Maddocks, **Scientific Editor** Benoît Dupont

To receive the latest issue and access back issues apply for a free membership at info@serene-risc.ca