Chapter 9
The Human Factor in Cybersecurity: Robust & Intelligent Defense

Julie L. Marble, W. F. Lawless, Ranjeev Mittu, Joseph Coyne, Myriam Abramson and Ciara Sibley

Abstract In this chapter, we review the pervasiveness of cyber threats and the roles of both attackers and cyber users (i.e. the targets of the attackers); the lack of awareness of cyber-threats by users; the complexity of the new cyber environment, including cyber risks; engineering approaches and tools to mitigate cyber threats; and current research to identify proactive steps that users and groups can take to reduce cyber-threats. In addition, we review the research needed on the psychology of users that poses risks to users from cyber-attacks. For the latter, we review the available theory at the individual and group levels that may help individual users, groups and organizations take actions against cyber threats. We end with future research needs and conclusions. In our discussion, we first agreed that cyber threats are making cyber environments more complex and uncomfortable for average users; second, we concluded that various factors are important (e.g., timely actions are often necessary in cyber space to counter the threats of the attacks that commonly occur at internet speeds, but also the 'slow and low' attacks that are difficult to detect, threats that occur only after pre-specified conditions have been satisfied that trigger an unsuspecting

W. F. Lawless (✉)
Paine College, 1235 15th Street, 30901, GA, Augusta, USA
e-mail: wlawless@paine.edu

R. Mittu · J. Coyne · M. Abramson · C. Sibley
Information Technology Division, Naval Research Laboratory,
4555 Overlook Ave SW, 20375 Washington, DC, USA
e-mail: ranjeev.mittu@nrl.navy.mil

J. Coyne
e-mail: joseph.coyne@nrl.navy.mil

M. Abramson
e-mail: myriam.abramson@nrl.navy.mil

C. Sibley
e-mail: ciara.sibley@nrl.navy.mil

J. L. Marble
Advanced Physics Laboratory Senior Human Factors Scientist Asymetric Operations Sector,
Johns Hopkins University, 11100 Johns Hopkins Road, Mailstop MP6 S334,
Laurel, MD 20723, USA
e-mail: julie.marble@navy.mil

S. Jajodia et al. (eds.), *Cyber Warfare,* Advances in Information Security 56,
DOI 10.1007/978-3-319-14039-1_9

attack). Third, we concluded that advanced persistent threats (APTs) pose a risk to users but also to national security (viz., the persistent threats posed by other Nations). Fourth, we contend that using "red" teams to search cyber defenses for vulnerabilities encourages users and organizations to better defend themselves. Fifth, the current state of theory leaves many questions unanswered that researchers must pursue to mitigate or neutralize present and future threats. Lastly, we agree with the literature that cyber space has had a dramatic impact on American life and that the cyber domain is a breeding ground for disorder. However, we also believe that actions by users and researchers can be taken to stay safe and ahead of existing and future threats.

9.1 The Cyber Problem

Introduction In our approach to cyber threats, we will review the increasing complexity of, and risks in, the new cyber environment. We will discuss cyber defenses and tools used in defenses, such as the use of engineering to mitigate cyber threats. More fully, we will review and discuss the pervasiveness of cyber-attacks from multiple perspectives: first at the individual level from the perspective of the human attacker and the user, the attacker's target; and second from the perspective of teams and organizations. We end with future research needs and conclusions.

Our Modern Digital Age We live and work in a digital age, where access to information of widely varying values is ubiquitous. However, users fail to comprehend the value of their personal information (e.g., birthdays, on-line browsing behavior, social interactions, etc.) to malicious actors. Information has always been important to survival; the original purpose of the internet was to share the information that would improve global social well-being (Glowniak 1998). The security of information has been defined[1] as "... protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction ..." Security directly describes how well a system is protected and indirectly the value of the information being protected (Lewis and Baker 2014). However in the modern digital age, sharing information now competes with protecting private information from unintended recipients; the complexity of security has increased to protect information that is deemed private, and the interaction between the complexity of networks and security defenses has led to increasing opacity in the functioning of networks and computers for typical users. Furthermore, as complexity increases with greater security features, systems and protocols, the "increased use of networked systems introduces [even newer] cyber vulnerabilities ..." (Loukas et al. 2013).

Digital space, or cyberspace, for our purposes consists of the three overlapping terrains as determined by Kello (2013, p. 17): (1) the internet (all interconnected computers); (2) the subset of websites comprising the world wide web accessible by only a URL; and (3) a cyber-archipelago of computer systems in theoretical seclusion,

[1] From 44 USC § 3542; see http://www.law.cornell.edu/uscode/text/44/3544.

separated from the internet. As Kello notes, these terrains imply that not all threats arrive from the internet, and the cyber-archipelago can only be attacked with access, which emphasizes the role of the human user and the potential for human error with the security of systems. This reduces the target space for malicious actors to access remote and closed targets, each susceptible to different exploits.

Martinez (2014) and others believe that the greatest cyber threats are internal threats from insiders; in particular both malicious dissatisfied actors as well as the unaware insider. Salim (2014), with data from Symantec Corporation's 2013 Internet Security Threat Report,[2] noted that 40 % of data breaches in 2012 were attributed to external hackers and 23 % to accidental data compromise by unaware users. However, for the 40 % of the breaches by hackers, it remains unknown how much of these breaches was due to manipulating users or defenders into an action that produced an exploit.

Cyber threats range over sources and types. For example spear-phishing emails typically target specific individuals or users, while malware is typically directed against websites or processes (e.g., Stuxnet). There are a varying range of malicious actors who work along a continuum of personal and ideological goals and intents, from individual actors, to hacktivists and on through to nation-state actors.

Social media is exploited by malicious actors who use it as a conduit to identify vulnerabilities and targets. Information gleaned from social media can be used to tailor spear-phishing and other exploits. Against the most common attacks (such as phishing email with malicious links or false advertisements that allow the download of malware), the typical defense is training people to "not to click", i.e., to just say "no". However, cyber space is too complex for simple "not to click" defenses; instead, as our arguments will show, multiple defenses that include modeling the cognitive decision-making of attackers and defenders are needed to mitigate the threats in this complex space.

Cyber threats can range from petty cybercrime (such as identity theft) to intense cyber war (for example, Russia's shutdown of media in Ukraine). However, petty crimes like identity theft can be leveraged as part of intense cyber war tactics, such as credit card theft to finance purchase of resources. In the cyber environment, asymmetric[3] capabilities magnify risk, threat and consequence arising even from a single actor; geographically distant adversaries can have significant real-world impacts with little effort and risk, expense or cost. Together, this means that cyber warfare is a new kind of war. After interviewing Pomerantsev, a journalist who wrote about cyberwar in a *Foreign Policy* article, the Washington Post (2014, 5/30) wrote:

> Traditional warfare is very expensive, requiring massive buildups and drains on the state treasury for military campaigns in far-flung locales. The new warfare will be cheap, low-intensity and most likely, waged primarily in cyberspace. Attacks will occur against economic

[2] www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid = istr-18.

[3] Asymmetry is a lack of symmetry; e.g., asymmetric warfare is war between belligerents whose relative military power differs significantly, or whose strategy or tactics differs significantly; retrieved from http://en.wikipedia.org/wiki/Asymmetric_warfare.

> targets rather than military targets. Taking down a stock market . . . has greater tactical value than taking out a hardened military target. . . . It is the ultimate asymmetric war in which we do not even know who to attack, or how or when.

Cyber warfare can yield "non-linear war" (Pomerantsev 2014), in which a smaller, geographically distant but highly capable opponent is able to have significant impacts on a much larger opponent; furthermore, due to the nature of the cyber environment, traceability of these actions can be limited. In August 2010, (Fox News 2010, 3/8) the U.S. publicly warned about the Chinese military's use of cyber-attacks run by civilian computer experts. These attacks were directed against American companies and government agencies, with the Chinese computer network, "Ghostnet", as one of several identified. The US alleged that these malicious military and civilian teams were developing computer viruses and other cyber capabilities to attack US infrastructure systems where vulnerable (Wall Street Journal 2009, 4/8).

Kello (2013, p. 39) cites Chairman of the Joint Chiefs of Staff Adm Michael Mullen's concern that the cyber tools under development in multiple nations may lead to a 'catastrophic' cyber event. The US is as vulnerable as any other nation or individual, causing the cyber domain to yield newly observable influences on patterns of rivalry (pp. 30–31). Concerning the individual impact of cybercrime, Lewis and Baker (2014) try to keep cyber threats in perspective: "Criminals still have difficulty turning stolen data into financial gain, but the constant stream of news contributes to a growing sense that cybercrime is out of control." While they estimate annual loses at $ 4–600 Billion, a fraction of one percent of global GDP, they go on to add that, today, effects of cybercrime are most notable in the shifts in employment away from highly valuable jobs, in part by damaging company performance and its impact to global growth through damage to national economies and to trade, competition and innovation.

Lewis and Baker (2014) caution that the financial losses may be even larger than they have reported because many cyber events go unreported for many reasons, including a desire to maintain face, protect intellectual property, and corporate privacy. In general, however, not only are most cybercrimes unreported, it is also not unusual for companies to suppress news they think reflects negatively upon them. Recently, for example, based on an internal investigation of General Motors' ignition switch recalls, Valukas (2014) found "a company hobbled by an internal culture that discouraged the flow of bad news". A company may ignore its own security warnings, as apparently occurred in the 2013 Target debit card hack. In this case, the FireEye detection system used by Target could have stopped the malware from acting to send out the stolen data. Apparently, in an instance of what is commonly called "human error", Target's security team turned that function off.[4] But that simplistic finding on the Target security team ignores the complexity of network architecture, and the difficulty of understanding the interactions between tools. Humans do not willingly set themselves up for failure, and generally take the actions that they perceive as

[4] See at http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

the most logical in the situation. However, there are few tools to support the performance of cyber defenders that can actively predict the consequences of actions or the emerging features of networks.

9.1.1 *Office, Home, and Online Shopping*

Cyber threats arise not only in the office, but also in the home, with social media, and with on-line shopping. For an example, Cisco reported[5] that 68 % of users surveyed said they had had computer trouble caused by spyware or adware; 60 % of those were unsure of their problem's origin; 20 % of those who tried to fix the problem said it had not been solved; and for those who had attempted to fix the problem, it cost on average about $ 129 per computer or to restore the system to a previous backup state. In many of these cases, it was simply cheaper to buy a new computer. Cleansing software programs are not always able to find root causes, implying that computer repair requires more technical expertise than the average user is capable. Even bigger problems loom with mobile electronic devices, such as smart phones.

Mobile users fall victim to malware via 'drive-by downloads'[6] from malicious sites, by downloading malware masquerading as desirable software such as an update, or offers for discount coupons and free games. An area of concern for mobile devices is the Quick Response (QR) codes available for users. These codes form a matrix barcode to store alphanumeric characters as a text or URL. A QR code can be scanned with a smartphone's camera as input into a QR reader's app. The QR code directs users to websites, videos, sends text messages and e-mails, or launches other apps. While convenient, the downside is that users are not aware of the content of a QR code until it has been scanned, increasing mobile security risks; further, many users are not aware of the potential commands that can be initiated by QR codes.[7] Malicious-attackers can use these codes to redirect users to malicious websites to download malicious apps that can, for example:

- Make calendars, contacts and credit card information available to cyber-criminals (Washington Post 2014, 6/13).
- Ask for social network passwords; once accessed, social networks can lead to sufficient personal information for identity theft.
- Track locations.
- Send texts to expensive phone numbers; e.g., in Russia (2013) an incident involved a mobile app titled "Jimm" that once installed, sent unwanted expensive texts ($ 6 each).

---

[5] see "Cisco cyber threat reports at http://www.cisco.com/c/en/us/products/security/annual_security_report.html/.

[6] "A drive-by download is when a malicious web site you visit downloads and installs software without your knowledge.", from http://www.it.cornell.edu/security/safety/malware/driveby.cfm.

[7] https://www.bullguard.com/bullguard-security-center/mobile-security/mobile-threats/malicious-qr-codes.aspx.

Recently there has been a rise in the occurrence of "ransom ware" by which a user downloads malware, that, when executed, encrypts the user's hard drive. The malware then notifies the user that in order to re-access the data on the computer, a ransom must be sent. One argument would be to engineer systems that are unbreakable, able to circumvent all attacks, such as credit card scams. But this explosion of engineered responses is untenable. For example, Salim (2014, p. 24) reported that building unbreakable credit card systems is not feasible when faced by resource and time constraints against attackers with ample time, money and protection by other nations. Not only is there a problem with credit cards, air traffic control and stock markets are also affected.

9.1.2 Air Traffic Control

The Inspector General[8] has warned that the U.S. Federal Air Administration's Air Traffic Control (ATC) system is unprepared for cyber threats:

> [In our] report on Federal Aviation Administration (FAA) web applications security and intrusion detection in air traffic control (ATC) systems. . . . We found that web applications used in supporting ATC systems operations were not properly secured to prevent attacks or unauthorized access. During the audit, our staff gained unauthorized access to information stored on web application computers and an ATC system, and confirmed system vulnerability to malicious code attacks. In addition, FAA had not established adequate intrusion–detection capability to monitor and detect potential cyber security incidents at ATC facilities. The intrusion–detection system has been deployed to only 11 (out of hundreds of) ATC facilities. Also, cyber incidents detected were not remediated in a timely manner.

Addressing ATC's failures, the Inspector General for the Department of Transportation (DOT) criticized DOT for failing to update IT systems as federally required. DOT's information systems are vulnerable to significant security threats and risks.

9.1.3 Stock Markets

Regarding stocks, Lewis and Baker (2014) conclude that "Stock market manipulation is a growth area for cybercrime." Making this threat clear, a hack of an Associated Press Twitter feed sent out a claim of an explosion at the White House, causing the stock market to tumble 100 points within a few seconds before it was identified as false.[9] A deeper concern, seemingly unrelated, is the claim by Lewis (2014) that

[8] "Quality control review on the vulnerability assessment of FAA's operations air traffic control system" (2011, 4/15), Project ID: QC-2011-047, from oig.dot.gov; quotes from FederalTimes (2014, 4/25), Government, industry target air traffic cyber-attacks", federaltimes.com.

[9] See at http://nymag.com/daily/intelligencer/2013/04/ap-twitter-hack-sends-stock-market-spinning.html.

millisecond "high-frequency trading" has rigged the stock market. Mary Jo White, Chairman Securities and Exchange Commission, denied that the market was rigged, noting that costs for common stocks had fallen.[10] Despite this incident, the White House requested funds from Congress "to help regulators cope with a technological revolution that has turned stock trading into an endeavor driven and dominated by fast computers".

Time-critical decisions are also an integral aspect to emergency first responders (Loukas et al. 2013) and to the Cyber Response Teams who may also have to fend off a cyber-attack during an emergency response. Based on models of quickening conflict escalation by Mallery (2011), Kello (2013, p. 34) warned:

> Consequently, the interaction domain of cyber conflict unfolds in milliseconds—an infinitesimally narrow response time for which existing crisis management procedures, which move at the speed of bureaucracy, may not be adequate.

9.1.4 Information Concerns

The *Washington Post* (2014) recently reviewed Vodaphone's report about the types of information being gathered by national governments:[11]

> Such systems can collect and analyze almost any information, including the content of most phone calls that flow over the Internet when it's not encrypted. As a result, governments can learn virtually anything people in their nations say or do online and frequently can learn where they are using location tracking, which is built into most cellular networks. The Vodafone report distinguishes between content—words or other information conveyed over its networks—and metadata, which reveals who is contacting whom and what kinds of communication systems they are using.

In its article, the Washington Post (2014) noted that cyber vulnerabilities are being built purposively into modern communication systems, including cell phones:

> Governments have been gaining increasingly intrusive access to communications for at least two decades, when the United States and other nations began passing laws requiring that powerful surveillance capabilities be built directly into emerging technologies, such as cellular networks and Internet-based telephone systems.

9.1.5 The Human Element

The human element is the common thread among all cyber threats. With malicious software, hackers exploit the motivation of users who are simply seeking to achieve

---

[10] *Washington Post* (2014, 6/6), "SEC aims to catch up to trading technology"; http://www.washingtonpost.com/business/economy/sec-aims-to-catch-up-to-trading-technology/2014/06/05/eee8ab06-ece0-11e3-b98c-72cef4a00499_story.html.

[11] http://www.vodafone.com/content/index/media/vodafone-group-releases/2014/law_enforcement_disclosure_report.html.

their goals (e.g., mundane goals like seeking a flight, ordering a book, or responding to an email). Hackers analyze the flow of users' tasks to determine where vulnerabilities can be found, then make decisions on what exploits to run based on their own malicious motivations and intents.

9.2 Overview: Our Approach to the Problem

In our review of cyber threats, we discuss the pervasiveness of cyber problems and the human role as both attacker and target; the lack of awareness by users; cyber defenses and tools; the complexity of the new cyber environment; engineering approaches to mitigate cyber threats; cyber risks; and current research along with theory at the individual and group levels. We end with future research needs and conclusions.

Recognizing the danger from cyber threats, the Federal Communications Commission (FCC) has quietly worked to expand its role among the federal agencies charged with defending the nation's networks from cyber-attack (Washington Post 2014, 6/12). The FCC's initiative follows a set of recommendations for businesses to bolster cyber-defenses issued by the National Institute of Standards and Technology (NIST 2014); NIST has also developed a framework for organizational structure and regulation to increase cyber security.

The classic response to cyber threats has been to focus on deterrence, implying the value of maintaining strong boundaries and increasing the cost of attacks. However, the common focus on deterrence of threats has led to scenarios where we run faster and faster to maintain the same position (i.e., Red Queen scenarios; discussed later) (Section 9.5.1). Consider for a moment password requirements: Kaspersky recommends 23 character passwords, comprising a mix of capital and lower case letters, numbers and special characters.[12] Accepting this recommendation puts an unwieldy cognitive burden on users, creating other vulnerabilities (e.g., recycled passwords, password 'safes'; etc.). Meanwhile, malicious actors informally try to understand the behavior of users even as institutional security policies attempt to limit the behaviors of users. These limits impact the ability of users to achieve their goals, forcing them to seek work-arounds, but yielding even newer vulnerabilities. To get in front of this situation with behavioral modeling, we propose that it is necessary to model the intents and motivations, the cognitions, of both malicious actors and users.

Usually the difference between an offensive and defensive response to a cyber-threat is very clear to both sides. However, notes Kello (2013 p. 32), sometimes a proactive defensive action can be mistaken by a malicious agent as an overt attack, causing the malicious agent to counter the defensive action, creating a cycle that spurs on the cyber arms race.

[12] See more at http://usa.kaspersky.com/products-services/home-computer-security/password-manager/?domain=kaspersky.com.

Continued reliance on engineered solutions to cyber incursions neglects a significant aspect of the problem. Okhravi et al. (2011)[13] note that in a contested environment, traditional cyber defenses can prove ineffective against a well-resourced opponent despite hardened systems. They recommend constructing a "moving target" for an active defense. The cyber domain is unique as a human developed environment, and while many tools used to exploit vulnerabilities in the environment are engineered, the selection of targets and implementation of defenses continue to rely on the ability of humans to understand the emerging complexities within this environment.

9.3 Cyber Problems are Pervasive

The breadth of the risks from cyber threats are sketched by Lewis and Baker (2014):

> Simply listing known cybercrime and cyber espionage incidents creates a dramatic narrative. We found hundreds of reports of companies being hacked. In the US, for example, the government notified 3000 companies in 2013 that they had been hacked. Two banks in the Persian Gulf lost $ 45 million in a few hours. A British company reported that it lost $ 1.3 billion from a single attack. Brazilian banks say their customers lose millions annually to cyber fraud.

9.3.1 Risks

Regarding the cyber risks posed to the average person, firm, and our nation, Axelrod and Iliev (2014) conclude that "(t)he risks include financial loss, loss of privacy, loss of intellectual property, breaches of national security through cyber espionage, and potential large-scale damage in a war involving cyber sabotage." Risk has been defined as a measure of the probability and severity of adverse effects (e.g., Lowrance 1976).[14] Applied to cyber threats, risk is the likelihood of a cyber-attack times the consequences of the losses expected from the attack.

Lewis and Baker (2014) note that targets are identified by attackers based on the value of the target and the ease of entry (risk equals consequence times probability; from Kaplan and Garrick 1981). However, given the complexity of cyber networks, the rise of emergent properties in these networks, and the evolution of technologies, it becomes very difficult for defenders and decision makers to provide risk assessments of their networks. What are needed are tools to help defenders understand the strategic value of their systems to attackers, and the risks from a loss of those systems once malicious actors have gained access.

---

[13] The authors are at MIT's Lincoln Laboratories.

[14] This definition comes from the University of Virginia's Center for Risk Management of Engineering Systems; more at http://www.sys.virginia.edu/risk/riskdefined.html.

The difficulty of attribution and prediction of the source (and therefore motivation) of opponents further reduces the ability of defenders to assess risk. Teams of malicious agents can amplify the risks from cyber weapons. Traceability in the cyber environment is difficult, and the anonymity lent by cyber increases the confidence of attackers. To magnify this even further, use of civilian 'militias' is increasingly common (Kello 2013). It is difficult to differentiate these militias from groups acting independently (e.g., Anonymous; see also New York Times (2014, 6/20)).

> Moreover, some countries—notably, Russia and China—increasingly employ cyber "militias" to prepare and execute hostilities. Such use of civilian proxies provides states plausible deniability if they chose to initiate a cyber-attack, but it also risks instigating a catalytic exchange should the lines of authority and communication break down or if agents decide to act alone.

Deception and subterfuge are common in the cyber-environment on the level of individual malicious actors as well as at the nation-state level. Attackers representing nation-states use cyber subterfuge to obtain the innovations they are unable to develop internally on their own (Lewis and Baker 2014), while others combine cyberwar tactics with traditional military strategies to achieve ends ranging from self-promotion to security. Use of deception in cyber exploits further reduces the ability of defenders to estimate risk. This is compounded when the 'average user' cannot foresee the potential impact of what appears to be a simple action (such as following a link in an email from what appears to be a trusted source, when that source has been hacked). Most users are unaware of the risks they face from deception and subterfuge.

9.3.2 Unaware Users

With the recent substantial growth in computing and internet use, the complexity of networks has expanded, increasing the opaqueness of how systems work. Few people know how their computers or the internet protocols work (e.g., who knows what TCP/IP actually does?). Nor are average users always fully aware of the risks arising from even simple actions (such as browsing the net).

It is not uncommon for a single user to have multiple devices; to be safe each device requires protection, implying that each user should have multiple aliases in the cyber environment. However, as Capelle (2014) notes, users take insufficient precautions to protect their data on their devices. He writes,

> . . . the Kaspersky-B2B International survey results show that close to 98 % of respondents use a digital device—smartphone, computer or tablet—to carry out financial transactions and 74 % regularly use e-wallets and e-payment systems. However, this increase in the use of mobile payments has not been accompanied by a change in users' security habits. Some 34 % of those surveyed stated for example that they took no security measures when using public WiFi networks, even though 60 % are not certain that the websites they use provide adequate protection for their passwords and personal data. This widespread lack of security reflexes is also evident when it comes to the software versions people use. Fully 27 % of users do not regularly update software on their devices, and so leave themselves open to recurring cyber-attacks.

Reason (2008) states that 'unsafe acts' in cyber can be seen as person-based; that is, arising from aberrant human cognitive processes, such as forgetfulness; or they can be considered from a system perspective. In the system perspective (of a human), humans are assumed to be fallible with errors to be expected. It is necessary for researchers to develop resilient defensive systems to protect against these errors. However, the increasing complexity of our networks increases the risks users face until acceptable defensive actions have been established. The commonness of malware also makes the perception of the impact of the consequence lower—malware slows digital devices, which is annoying; but the perception that users could experience identity theft is underestimated.

These errors can be catastrophic. Kello (2013, p. 23) provides an example of a warning based on a simulation of power-failure in the USA:

> Based on extrapolations of a cyber-attack simulation conducted by the National Academy of Sciences in 2007, penetration of the control system of the U.S. electrical grid could cause "hundreds or even thousands of deaths" as a result of human exposure to extreme temperatures (National Research Council of the National Academies 2012).

This warning was realized within a (Wall Street Journal, 2009, 4/28).

9.3.3 Malware Origination, Repair and Deception

The prevalence of malware makes it difficult to determine where a problem originates; if users cannot figure out the origination of cyber threats, can they be prevented? Attacks against 'average users' often uses deception to gain access. Malicious actors develop malware that leverages deception, requiring exploiters to develop an understanding of user defensive tasks, user decision processes, and a malicious agent's ability to view across the entirety of the network they aim to exploit, for example through impersonation of trusted sources. However, strategic deception is also used in exploits against larger corporate entities. From the media comes an example of the deceptions and misdirection used by criminals acting against banks (USA Today 2014):

> To draw attention away from the massive [money] transfers, the hackers often created a diversion, such as a "denial of service" attack that would bombard the website with traffic in an attempt to shut it down, the law enforcement official said. While the business scrambled to protect its portal, the hackers would push the wire transfer through unnoticed for hours, the official said. By the time the bank realized the money was missing, the hackers had laundered it through so many accounts it became untraceable.

Deception Drones are a new element in US aviation (Los Angeles Times 2014, 6/10). Depending on their mission, they are vulnerable to cyber-attack from novel vulnerabilities. Hartmann and Steup (2013, p. 22): "Events such as the loss of an RQ-170 Sentinel to Iranian military forces . . . [illustrate, possibly, that]:

> . . . a vulnerability of the UAV sensor system with effects on the navigation system was used to attack the GPS system. . . . The GPS-satellite-signal is overlaid by a spoofed GPS-signal

originating from a local transmitter with a stronger signal. The spoofed GPS-signal simulates the GPS-satellite-signal, leading to a falsified estimation of the UAVs current position. Supporters of this theory suppose that Iranian forces jammed the satellite communication of the drone and spoofed the GPS-signal to land the drone safely on an Iranian airfield.

9.3.4 Threat Sources

Threat sources have a wide range, from individual malicious agents and the tools used in attacks against users to nation-state actors running advanced persistent threats over long time frames. Criminal hackers and foreign cyber attackers probe for weaknesses in individuals, firms or institutions in a malicious attempt to understand user goals, motivations, intents and behaviors. Emerging vulnerabilities represent an opportunity to exploit a potential resource. From Axelrod and Iliev (2014), "New vulnerabilities in computer systems are constantly being discovered. When an individual, group, or nation has access to means of exploiting such vulnerabilities in a rival's computer systems, it faces a decision of whether to exploit its capacity immediately or wait for a more propitious time." Vulnerabilities arise from the complexity of networks, and the inability to comprehend the properties from complex interactions, and the human user and defender is lacking the tools to predict from where the next threat will arise.

From a boundary maintenance perspective, cyber criminals seeking vulnerabilities in a target organization's boundaries try to mount attacks without wasting resources by attacking at the points of weakness that they have identified; yet with the low cost of each, multiple attacks may be mounted simultaneously, obscuring the state of the system or the source of an attack to defenders. Vulnerabilities are found by an exploration of a team's or an organization's boundaries, but also, based on interdependence theory, by perturbing a team or an organization to observe how a target behaves inside and outside of its established boundaries (see Section 9.7.5). This is done by malicious agents in order to understand user decisions and responses. Sun Tzu was adapted by Symantec into a quote as "Cyber Sun Tzu" to thwart the legions of cybercriminals we face today (New York Times 2014, 6/21), but it is as true of the tactics utilized by malicious actors against targets: "when the enemy is relaxed, make them toil; when full, make them starve; when settled, make them move."

We ignore the human element of cyber threats at our peril. Cyber threats arise from engineered tools designed to exploit the vulnerabilities of users; the tools are used by intelligent adversaries with a variety of motivations, intents, and goals. Kello (2013, p. 14) points out that vulnerabilities to threats arising from new technologies are often ignored or dismissed because of a failure to grasp the full source or impact of the threat:

Historically, bad theories of new technology have been behind many a strategic blunder. In 1914, British commanders failed to grasp that the torpedo boat had rendered their magnificent surface fleet obsolescent. In 1940, French strategic doctrine misinterpreted the lessons of mechanized warfare and prescribed no response to the Nazi tank assault. The cyber revolution

> is no exception to this problem of lag in strategic adaptation. . . . Circumstances in the lead-up to the U.S. offensive cyber operation known as "Olympic Games," which destroyed enrichment centrifuges in Iran, vividly demonstrate the problem. The custodians of the worm (named Stuxnet by its discoverers) grappled with three sets of doctrinal quandaries: (1) ambiguities regarding the tactical viability of cyber-attack to destroy physical assets; (2) concerns that the advanced code would proliferate to weaker opponents who could reengineer it to hit facilities back home; and (3) anxieties over the dangerous precedent that the operation would set—would it embolden adversaries to unleash their own virtual stock-piles?

While the computer science problems of cyberwar are significant, the human user remains the primary weak link. For example, phishing, spearfishing, spyware, malware, key loggers; attacks made through wi-fi;[15] attacks via mobile phones; email hacking and attacks through linked accounts; use of social media for distributed denial of service attacks; and the use of social media for crowd agitation campaigns to promote hacking of government, military and other agencies. In many respects, these combine to make for a new kind of warfare.

9.4 The Complex Cyber-Environment

Cyber defense in a complex cyber environment is not straightforward. We must realize we are in a war waged across a new terrain and confronted by a new enemy, reducing our likelihood of success. From Sun Tzu (Giles 2007), "If you do not know your enemies nor yourself, you will be imperiled in every single battle." Let's begin by exploring the enemy's battle terrain.

9.4.1 Cyber-Layers

Cyber security and cyber-defense have multiple levels, or strata, of interconnectivity, forming multiplicative relationships between aliases, people, and locations.[16] Malicious agents can target any of the multiple levels. The lowest level is geographic, then the physical infrastructure, the information layer, cyber identity layer, and people layer. The geographic layer on the bottom and the person layer on the top are familiar and are usually combined for military planning operations. The three middle layers are much more fluid and complex. These three layers are continually morphing, advancing and obfuscating. In its layer, information may be shared or unique to identity; people may have multiple cyber identities that can be easily linked or not. The content of a network resides on the information layer. The content consists of email

[15] Problems exist with free wi-fi connections. An article in the *New York Times* (2014, 6/4) hoped to protect travelers using free wi-fi: "Make sure that any site you visit has 'HTTPS' in front of the URL; Use a virtual private network, or VPN; Sign up for two-step verification; and Bring only what you need and turn off what you're not using.'

[16] Some of these ideas come from NSA: http://www.nsa.gov/ia/_files/support/defenseindepth.pdf.

messages, files, website, or anything electronically stored or transmitted. The Physical Infrastructure layer represents the physical hardware of cyberspace, the fiber-optic cables, satellites, routers, servers, etc. We discuss the cyber identify layer next.

9.4.2 Malicious Agents

The Cyber Identity layer is probably the most complex. It is how entities are identified on the network. This can be an individual user represented by multiple points of presence, i.e., personal phone, work phone, multiple email addresses, printer, fax, website, blog, etc. Consider that one individual with multiple, complex relationships accessing other levels of the environment can send anything over the internet to any location in the world. However, for most typical users, cyber identities (aliases) are easily linked.

Networks are built for ease of communications, not for security; an inherent design vulnerability. While we are easily able to connect new and different technologies to the net (e.g., homes; cars; weapons), we often do so with minimal concern for securing the network. The convergence of technology and the increasing complexity of these networks pose the challenge of identifying malicious agents and maintaining the situational awareness about their presence on networks.

9.4.3 Social Media

Malicious actors can, and do, leverage social media to gain insight into our behavior. At home (Carley et al. 2013), social media can be leveraged by malicious agents to influence user behaviors in a way that is an indicator of the roles these malicious actors want users to play as part of a staged event, serious enough to warrant an FBI rapid response.[17]

Further emphasizing the need to model human behavior and cognition for vulnerabilities, recent work by Trendmicro[18] indicated that 91 % of hacks begin with some form of phishing. They went on to report that targeting starts by 'pre-infiltration reconnaissance' where individuals are first identified and then profiled via information posted on social networks and the organizations' own websites. Thus, the attacker constructs an email tailored to the target, compelling enough that the target will open the attached file and get infected, most likely with a remote access tool (RAT; also, RATrojan) (Washington Post 2011, 8/3).

---

[17] e.g., from FBI Testimony, a malicious agent was charged with "wire and bank fraud for his role as the primary developer and distributor of the malicious software known as Spyeye"; http://www.fbi.gov/news/testimony/the-fbis-role-in-cyber-security.

[18] See http://www.infosecurity-magazine.com/view/29562/91-of-apt-attacks-start-with-a-spearphishing-email/.

9.5 Engineering Approaches

9.5.1 Red Queen

Engineering approaches to mitigating cyber-threats have led to an arms race. To quote Lewis Carroll, "It takes all the running you can do, to keep in the same place."[19] A never ending arms race means that defenders are always playing catch up, requiring: stronger protocols; stronger encryption; more rigorous password management; automated patching; firewalls; defense-in-depth; intrusion detection systems; and anti-virus software. Yet, the building and maintenance of engineered techniques do not address the most fundamental threats of cyberspace, those arising from human performance.

9.5.2 Blaming Users

The fundamental issue is seeing cyber-security as a problem of computer science and information technology while neglecting the impact of system complexity on users. Cyber-attacks are often called "human" engineering. The common perception from the human engineering perspective is that cyber-security is caused by a lack of discipline, when it is really a cognitive science issue. The typical solution is to blame users, shame them and retrain them; i.e., with case-based solutions. However, the solutions proffered rely on increasingly frustrating and difficult policies implemented at work for each new case, suggesting a lack of teamwork between cyber defenders and users (cf. interdependence theory). Worse, these solutions seldom prevent or uncover new vulnerabilities and new attacks that further exploit cognitive vulnerabilities.

9.5.3 Fulcrum of Power

Users, cyber defenders and malicious actors form a fulcrum of power (Forsythe et al. 2012): Defenders control user behavior through policies and software limitations when they should be limiting the behavior of malicious agents through modeling and prediction (e.g., with Artificial Intelligence, or AI). Users may be unaware of, or indifferent to, the potential sources of risk that they are being protected from by these policies (due to a lack of understanding of the risk consequences); dissatisfied by the agencies that defend them (potentially creating a malicious insider threat); or dissatisfied by the limits a policy places on their ability to perform their job.

[19] i.e., Carroll's The Red Queen, in "Through the Looking Glass".

The ability of users to understand the risks they face may be limited due to a lack of communication (e.g., Cisco's[20] report indicated users were often unaware of their organization's security policy), the technical complexity of the network and its sources of risk, or because their work and operations have a higher priority to them in the short term. Security measures may limit or irritate users, causing them to bypass security settings and often inadvertently result in security incidents (e.g., using USB memory sticks). In contrast, those known as "cyber defenders" are more security aware, more able to maintain a smaller cyber footprint, and more likely to follow their organization's policy due to a greater sensitivity to the cyber threats and risks that they face. At work or at home, cyber defenders maintain the sense of vulnerability, leading them to view workable security measures as necessary, a best practice for all users.

From Kello (2013, p. 28), "Therein lies the root dilemma of cyber-security: an impregnable computer system is inaccessible to legitimate users while an accessible machine is inherently manipulable by pernicious code."

9.5.4 User Vulnerability

Within a cyber-network, we argue that the human user is both the greatest source of vulnerability and the greatest resource for a defense. Cyber threats pose a new kind of war where personal information needs to be seen as an asset (not just data) to be protected (NIST 2010). In a newly emerging version of an old threat (recall the PC Cyborg/AIDS Trojan from 1989), accessed by typically entering the system via a downloaded file, then vulnerable personal information or files may be locked away by cybercriminals from users. The New York Times (2014, 6/21) describes how this works:

> Cybercriminals are ... circumventing firewalls and antivirus programs ... [and] resorting to ransomware, which encrypts computer data and holds it hostage until a fee is paid. Some hackers plant virus-loaded ads on legitimate websites, enabling them to remotely wipe a hard drive clean or cause it to overheat. Meanwhile, companies are being routinely targeted by attacks sponsored by the governments of Iran and China. Even small start-ups are suffering from denial-of-service extortion attacks, in which hackers threaten to disable their websites unless money is paid.

Kello (2013, p. 30) tried to highlight the difficulty of defending against cyber-attacks:

> The enormity of the defender's challenge is convincingly illustrated by the successful penetration of computer systems at Google and RSA, two companies that represent the quintessence of technological ability in the current information age. (In 2010, Google announced that sophisticated Chinese agents had breached its systems, and in 2011, unknown parties compromised RSA's authentication products. This was followed by attempts to penetrate computers at Lockheed Martin, an RSA client.)

[20] see "Cisco cyber threat reports at http://www.cisco.com/c/en/us/products/security/annual_security_report.html.

Kahneman's (2011) philosophy of mind explains cognitive vulnerabilities by the duality of human thought processes. On the one hand, our associative mind jumps to conclusions by continuously looking for patterns even where none exists; on the other hand, our reasoning self requires concentration and effort to make decisions. The principle of least effort (Zipf 1949) underlies most human judgment and habits, both good habits and bad ones. We quickly develop habits as shortcuts because reasoning takes too much time and effort. Habits make us predictable and vulnerable. As the complexity of our interactions in cyberspace increase, so will our reliance on habits, motivating malicious agents to learn those habits most vulnerable to exploitation.

9.6 Intelligent Adversaries

9.6.1 Changing Tools and Techniques

McMorrow (2010, p. 14) concluded that "[I]n cyber-security there are adversaries, and the adversaries are purposeful and intelligent." The techniques used by malicious actors are constantly changing. As demonstrated by the success of "Cosmo the god", who excelled in creating new disguises for exploits.

> Over the course of 2012, Cosmo and his group UG Nazi took part in many of the highest-profile hacking incidents of the year. UG Nazi, which began as a politicized group that opposed SOPA,[21] took down a bevy of websites this year, including those for NASDAQ, CIA.gov, and UFC.com.[22] It redirected 4Chan's[23] DNS to point to its own Twitter feed. Cosmo pioneered social-engineering techniques that allowed him to gain access to user accounts at Amazon, PayPal, and a slew of other companies. He was arrested in June, as a part of a multi-state FBI sting (Wired 2012).

9.6.2 Using Deception for Defense

There are only so many ways you can deceive and ultimately each new technique is an old technique in new clothes. Yet, there are still users who respond to 'Ethiopian lottery' email.[24] From Sun Tzu (Giles 2007, p. 18), "All warfare is based on deception. Hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near." As Axelrod and Iliev (2014) claim:

---

[21] Stop Online Piracy Act (SOPA); see http://en.wikipedia.org/wiki/Stop_Online_Piracy_Act.
[22] Ultimate Fighter: see http://www.ufc.com.
[23] An imageboard site; see http://www.networkworld.com/article/2222511/microsoft-subnet/hacktivists-ugnazi-attack-4chan-cloudflare-and-wounded-warrior-project.html.
[24] For a review of lottery and other e-scams, see http://www.fbi.gov/.

> The Stealth of a resource is the probability that if you use it now it will still be usable in the next time period. The Persistence of a resource is the probability that if you refrain from using it now, it will still be useable in the next time period.

To get ahead of the behavioral modeling of the malicious agents who attempt to exploit users, we need a cognitive model of malicious attacker(s).

9.7 Current Research

9.7.1 Theory

In this section, as applied to cyber threats and cyber defenses, we review the cognitive science of individual behavior, cognitive structures for the individual, and unanswered questions for applying cognitive science to individuals in the cyber domain. Second, we review the theory of interdependence to better understand and predict the behavior of teams and organizations and the unanswered questions for interdependent states. Third, we review what is known and not known about communication among teams. We end this section by noting that research is needed on leveraging cognitive models to predict how a malicious agent's motivation and intent influence their selection of a tool to exploit a user.

Behavioral theory is either based on traditional individual methodological perspectives (e.g., cognitive architectures) or, but less often, on groups (i.e., interdependent theory). Methodological individualism assumes that individuals are more stable than labile irrespective of the social interactions in which they engage (Ahdieh 2009). Interdependence theory assumes the opposite, that a state of mutual dependence between the participants of an interaction affects, or skews, the individual beliefs or behaviors of participants; i.e., interdependence changes preferences, no matter how strongly held (Kelley 1992). Further, given the anonymity allowed by the cyber environment, cyber aliases allow for significantly different behaviors as a function of the community surrounding an alias (e.g., when a malicious agent poses "to be from the FBI Director or other top official, it is most likely a scam"[25]).

If the problems with behavioral theory can be solved, then, technological solutions may become feasible. According to Martinez (2014, p. 2) ". . . the interplay between the human and the machine is paramount to reach timely decisions . . . [by] reduc[ing] the information entropy to reach actionable decisions." He believes that one solution "is to identify an architecture that is suitable for machine learning techniques to enable important augmented cognition capabilities in the context of complex decision support systems."

[25] http://www.fbi.gov/scams-safety/e-scams.

9.7.2 Attribution

The attribution problem, or identifying the sources of cyber threats, is one of the major defense challenges in cybersecurity due to the pseudonimity of cyberspace. Current cybersecurity efforts are directed toward technical attribution in the development of the black lists of malicious hosts in order to block the propagation of malicious packets and URLs. However, a gap exists between technical and human attribution because malicious software can execute from a remote host. Furthermore, malicious actors exchange, buy, and sell code to be retooled and rewritten, complicating the attribution problem. It is during the reconnaissance phase of an attack, however, that an attacker is most vulnerable to human attribution because of repeated interactions, external or internal, with a target host (Boebert 2010). Detecting malicious intent during an "external" reconnaissance is however a hard problem due to the serendipity of Web browsing. For example, an innocent person might stumble upon a honeypot thereby creating a false positive. Machine learning techniques for authenticating and modeling users in cyberspace from the history of their digital traces address the attribution problem from a behavioral perspective (Abramson 2013, 2014). Current challenges include malicious intent understanding from user interactions in cyberspace.

9.7.3 Cognitive Architectures

Eventually, it may be possible to use cognitive architectures to predict the next moves of malicious actors and agents (e.g., by detecting Advanced Persistent Threats, or APTs,[26] often directed by a government, like espionage by the Chinese and Russians, or the disruptive-Stuxnet by the Americans). Cognitive Science may be useful as a tool to connect media and behavior. Cyberspace is a complex ecosystem requiring a multi-disciplinary scientific approach. By understanding the decision making process, the motivations, and intents of malicious actors, it may be possible to predict the selection of exploits based on the goals of the malicious actor. Conversely, understanding decision processes, motivation and intent may be useful to differentiate the signal of a malicious actor from the false alarms inherent within networks.

Interdisciplinary Once we have identified the human behavior and motivations for a cyber-attack, numerous models exist with different applications, strengths, and utilities. We propose that the first step is to determine what we want to know, and explore the models able to provide that insight. The U.S. Navy explored this problem last year:[27] "Develop and validate a computational model of the cognitive processes from

[26] See en.m.wikipedia.org.
[27] Cognitive Modeling for Cyber Defense. Navy SBIR 2013.2. Topic N132–132. ONR; see http://www.navysbir.com/n13_2/N132-132.htm.

cues to actions of the attackers, defenders, and users to create a synthetic experimentation capability to examine, explore, and assess effectiveness of cyber operations."

Behavioral Intent Analysis The characteristics of the network can be thought of as stimulus cues (e.g., Feldman and Lynch 1988). To make sense of, and predict, the environment, humans attempt to find patterns in stimuli. Patterns of the type and number of cues from stimuli yield a belief about the current environment (i.e., a 'guess' or inference about a system's state). Each belief will prime associated motivations that compete against each other (Bernard and Backus 2009). The motivations that will become activated are those with the strongest congruence between the respective motivation and the attitude towards it; those associated with the perceived social norms that favor the motivation; and those where the perception that the action associated with a motivation can be carried out.

An activated motivation primes certain potential intentions (Bernard and Backus 2009). Primed intentions become active when cues supporting the respective intentions are present. Each activated intention primes associated potential behaviors. The potential behavior(s) that ultimately becomes activated is a function of the type and degree of associated affect (positive or negative) and the activated perception. That is, an entity may have an intention to do something, but how the intention is specifically carried out depends, in part, on the emotional state at that point in time.

If we knew the cues affecting a malicious agent, then, based on the types of data being protected, we could infer a set of behavioral intents. If we then applied a model of human cognition to our model of the malicious agent, we could use it to choose from the possible set of exploits. These steps could help us to create a tool that, while not identifying all of the attacks possible, could reduce the uncertainty in the cyber battlespace by identifying for further exploration those cues indicative of specific exploits (e.g., with AI). For example, one way that firms on their own are attempting to identify attackers is with active defenses: From the New York Times (2014, 6/21):

> . . . more companies are resorting to countermeasures like planting false information on their own servers to mislead data thieves, patrolling online forums to watch for stolen information and creating "honey pot" servers that gather information about intruders.

We need the development of programs to train users in cognitive defenses against cyber-exploitation and attack. We need multi-layered complex adaptive system models to train users in "cyber-street smarts" to recognize vulnerabilities, attacks, exploitations and suitable defenses. Lastly, we need to develop new "crowd-self-policing" techniques for cyber environments. We should also explore: "Who is vulnerable to what kinds of deception?"; "What makes good deception?" and "How can we detect deception?"

9.7.4 Cyber Security Questions

We argue that the following list represents the key cyber-security questions that need to be answered to address behavioral intent analyses:

Pursued from the Human Dimension:

- How do we measure performance in the cyber domain?
- What factors underlie cyber situation awareness?
- What cognitive and personality attributes characterize better cyber analysts?
- How do we train cyber defenders to be effective?
- What fidelity level is required for effective training?
- What are the characteristics of deception?
- Can we devise a test to discriminate between cyber defenders and ordinary users?

In addition, we provide a list of needed research tools:

- Behavioral modeling of vulnerabilities;
- Cognitively compatible semantic representation of cyber data and system state;
- Autonomous aids to identify situation awareness and the detection of deception; and,
- Communication aides (identifying the information propagating through social media).

9.7.5 Interdependence Theory

Until now, we have addressed cyber threats primarily from an individual perspective. Methodological individualism (e.g., game theory, psychology, learning) focuses on changing the individual in the hope that it may change society (Ahdieh 2009); but methodological individualism has serious shortcomings. For example, game theory remains unproven (Schweitzer et al. 2009). Some of game theory's strongest adherents admit that it is not connected to reality (e.g., Rand and Nowak 2013); yet, despite this disconnect, game theorists conclude that cooperation produces the superior social good (Axelrod 1984), a conclusion supported by a recent review on the theory of human teams (Bell et al. 2012).

That individualism and cooperation do not account for attacks on an organization's boundaries is not surprising. What surprises is how little the traditional focus on individuals has to offer to the science of real organizations. To address cybersecurity from an individual perspective cannot begin to account for the extraordinary time, energy and personnel real groups and organizations devote to defend themselves against all forms of real competition, including cyber-attacks. That is why we continue to develop the theory of interdependence to account for the irrational effects from the interdependence between uncertainty and the incompleteness of meaning that serves to motivate competition (Lawless et al. 2013). In the process, we discover that a large part of the problem with existing social-psychological theory is its overfocus on the individual, especially where it assumes that social reality and cognitive factors are constituted of logically independent and identically distributed (iid) elements. Consequently, through the lens of interdependence, the critical ingredient in group behavior, we can not only study how groups in reality defend themselves, but

also, and surprisingly, by unifying theories of cognition and behavior, we can begin to open an unseen window into the individual.

Organizations are systems of interdependence (Smith and Tushman 2005); social behavior is interdependent; and the interaction is characterized by interdependence (Thibaut and Kelley 1959). Interdependence theory was derived from game theory; it was formalized by Thibaut and Kelley, but later abandoned by its surviving author (Kelley 1992); Kelley had been unable to explain why subject preferences, no matter how strong, collected before games were played differed from the actual choices made by subjects during games. Nor has game theory fared well (Schweitzer et al. 2009); even its leading proponents admit that it has no ground truth, that games are not "a good representation of [our] world" (Rand and Nowak 2013, p. 416). Furthermore, no theory of organizations has yet been accepted (Pfeffer and Fong 2005). To counter this weakness in individualism, in this review, we will present the outline of a theory of interdependence.

The topic of deception is integral to cybercrime and offers a natural segue into interdependence theory, built around the idea that all perception leads to a belief that is a construction of reality, an illusion, or, more likely, a combination (Adelson 2000); that physical reality is orthogonal to imagined reality; and that the illusions (or errors) in the beliefs about reality allow challengers to compete against another's construction of reality, thereby generating social dynamics (Lawless et al. 2013). In contrast to the belief in a stable view of reality contingent upon the independent, identically distributed (iid) elements supposedly underpinning situational awareness, the multiple interpretations of reality that commonly arise are derived from socially interdependent situations; instead of stability, interdependence is simulated by a simple bistable image or function. Interdependent states are associated with high levels of uncertainty, indicating that unknowns outweigh ground truth; overriding this uncertainty, as Smallman (2012) has concluded, can produce tragic mistakes.[28] To address this uncertainty for well-defined situations, as in purchasing goods, humans establish social, cultural and legal rules to guide their behaviors. To address the uncertainty arising from ill-defined or poorly defined situations requires teams competing against each other, creating bistable perspectives (e.g., the debates commonly presented before audiences).

Bistability implies the possibility of tradeoffs as teams, groups or organizations make decisions; it is exemplified by scientists arguing over the correct interpretation of data, by politicians arguing over the interpretation of polls, and in the courtroom by attorneys arguing over the facts of a case; e.g., in the latter case, two bistable perspectives are reconstructed before a neutral jury as the two sides help the jury to work through the biases in the opposing perspectives until the better perspective is selected by the jury (Freer and Perdue 1996).

In the bistable view, a state of mutual dependence changes the statistics of interaction, confounding individual effects (Lawless et al. 2013). As with groupthink, teams reduce the degrees of freedom important to independent statistics, resulting

[28] E.g., the USS Greenville tragedy in 2001 that broke apart and sunk a Japanese tour boat.

in more power to statistical analyses than should be allowed (Kenny et al. 1998). Team members cooperate to multitask in a state of interdependence (Smith and Tushman 2005). But to multitask, team structures are built with heterogeneous roles of specialists, generating less entropy than a collection of individuals performing the same actions. Why? Interdependence causes a loss in statistical degrees of freedom (dof; see Kenny et al. 1998). Given entropy, S, for $S = k \log W$, as interdependence increases, W decreases, reducing entropy; i.e., S is proportional to $\log W \approx \log (dof)$. Consequently, given $A = U\text{-}TS$, where A is the available energy, U the internal energy, T the temperature, S the entropy, and TS is the energy not available for more work, then the free energy available increases for the structure of a team, a firm or a system to do needed work. Thus, the structure of a well-performing group generates less total entropy than the equal number of individuals performing the same set of tasks (similarly, a heterogeneous cloud is more cost-effective at providing specialized services matched to user needs; in Walters 2014). That is, the structural costs for a team to operate (e.g., coordination paths) are less for the set of individuals who are members of a team than the same individuals working as individuals, the impetus across a weakened market that drives two competitors to merge into a cooperative structure to survive (Lawless et al. 2013). With this information, we can distinguish good and bad team structures. Interestingly, the distinguishability of agents diminishes as the interdependence among them increases.

Assume that a primary goal of living organisms is to survive (Darwin 1973; Kello 2013). Assume also that individuals multitask poorly (Wickens 1992), but that groups perform better than individuals with members performing specialized tasks (Ambrose 2001). Next, assume that well-performing multitasking groups perform better than individuals (Rajivan et al. 2013). Then, if we construe a functional group (e.g., team, firm) as the mechanism that best gathers the resources (energy) needed to survive, in order to minimize entropy losses caused by group formation (Lawless et al. 2013), boundary maintenance becomes an integral factor in survival (Lawless et al. 2014). Unlike low entropy for the formation of best teams, when compared to low-performance teams, we expect that the best performing teams are signified as those that generate maximum entropy, making them more efficient and stable; we do not discuss this further at this time; but see Pressé et al. 2013.

Boundary maintenance entails defending against the threats to a group, including by responding to the risks of cyber threats; viz., the use of "shaming" indicates poor teamwork in the maintenance of their team's boundary. As wealth increases, the maintenance of boundaries becomes stronger. That is, according to Lewis and Baker, "Wealthier countries are more attractive targets for hackers but they also have better defenses. Less-developed countries are more vulnerable." Generalizing, the better a team performs the stronger becomes its boundary.

Predictions and Assessments Interdependence theory provides a platform for team, organizational, and system predictions and assessments. But, according to interdependence theory, when social agents confront ill-defined problems in states of interdependence, the information derived from them is forever incomplete (Lawless et al. 2013); that is, the information that can be collected from both sides of an

interdependent state cannot be used to reconstruct the original state. When outcomes are unpredictable in, say a court, the best result for justice is when legal adversaries in a courtroom are not only competent, but have equal skills and equal amounts of self-interest at stake in the outcome of a trial (Freer and Perdue 1996), exactly the condition for what makes prediction difficult, not only for courtrooms, but with competitive political races, revolutionary science, etc. Thus, in a cyber-exploit, as with any other attack scenario, attackers prefer not to oppose equally capable opponents, at least without some form of advantage (surprise, new weapons or tactics, etc.).

For example,[29] the US Navy, US Marine Corps and the US Coast Guard want to maintain control of the seas. In order to accomplish this goal, they describe "how seapower will be applied around the world to protect our way of life, as we join with other like-minded nations to protect and sustain the global, inter-connected system through which we prosper."

We have studied predictions made under states of interdependence in competitive situations to conclude that they are neither reliable nor valid. However, these predictions become more reliable and valid once an argument has shifted to favor one protagonist over another, thus, ending the state of interdependence, but maybe prematurely when the uncertainty remains high. The message is that the information generated by the interdependence associated with conflict may indicate a problem exists that has yet to be solved.

This phenomenon is more common than recognized. The outcome of the Clinton-Obama competition for the Democratic Nominee for the US Presidency was unclear during January 2008; the matter had been decided by February 2008.[30] Similarly, as of June 2014, predictions for control of the US Senate are no better than 50–50 % for either the status quo or Republican control.[31] If states of interdependence reflect limit cycles (Lawless et al. 2013), then one explanation for the high-levels of uncertainty that may exist comes from the conclusion by Chakrabarti and Ghosh (2013) that the net entropy production (information) for limit cycles is zero.

Interdependence theory poses several new questions:

- How do members of a team during its structural formation align their behaviors to build a group that multitasks better; does structural formation indicate the existence of specialized roles for a team's mission?
- Can we establish, mathematically, the minimum number of members of a team necessary to perform a mission or to defend a firm against a cyber-attack?
- What team characteristics define effective cyber incident response teams?
- Can we develop a tool to measure team performance (Psychophysics and psychometrics; Communication models; entropy heat maps)?
- Can teams be controlled to solve the problems they confront while minimizing mistakes when under competitive threats posed, say, by cyber-attacks?

[29] From US Navy, US Marine Corps and US Coast Guard (2007), "A cooperative strategy for 21st Century seapower http://www.navy.mil/maritime/maritimestrategy.pdf.
[30] See the Iowa Electronic Market; www.biz.uiowa.edu/iem/index.cfm.
[31] *Ibid*.

- Do individuals organize best by pooling resources into autonomous groups like teams and firms—Does self-organization lead to better defenses against cyber-attacks?
- What does an organization need to be able to predict its trajectory and assess itself? Viz., which organizations can predict their trajectory? This assumes a leader, but arguably, entities outside of the nation-state do not have a set leader or even set goals (again, Anonymous; see also New York Times 2014, 6/20). Others, like the old Chaos Computer Club did have goals and agendas but individuals still appeared to work consensus style.
- From a theoretical perspective, can a tool be devised to distinguish between good and poor performing teams (e.g., metrics for efficiency; stability; also, considerations of least and maximum entropy)?

9.7.6 Communication Among Teams

Teams organize around multitasking, which requires cooperation among other attributes (Lawless et al. 2013). From the perspective of static self-reports taken after a decision-making event, the larger the group involved in making a decision, the more interdependent it becomes (Lawless et al. 2014); from the perspective of information theory, a team attempts to maximize the flow of information into and out of its team interdependent with the environment by increasing its adaptivity, by minimizing its internal computations on the information flow, and by maximizing the relevance of its response to the environment.

What Makes for Good Teams Little is known theoretically about what makes for a good team (Bell et al. 2012). Based on small-group studies in the laboratory, good teams communicate together well. Good teams have experienced teammates, underscoring the value of training (Lawless et al. 2013); when joined by a new teammate, a team's performance is disrupted for a period, no matter how proficient is the new member (Bell et al. 2012). The better groups prefer to be cooperative rather than adversarial. However, from the study of the best performing teams away from the laboratory, Hackman (2011) found that the best teams often experienced conflict over issues of disagreement, but that once these issues were worked out, it led them to more creative results.

If the purpose of a team is to multitask (Lawless et al. 2013), thereby giving it more power when the team's [multitasking] actions are united, the mistakes made by a team potentially may be of a larger magnitude than those made by an equal number of independent individuals (e.g., from convergent group biases, like groupthink). Feedback becomes important to help a team act in response to a mistake. To minimize mistakes, the best feedback occurs in settings where challenges are permitted, where mutual self-interests of challengers are at stake (as has been concluded for justice to be served; in Freer and Perdue 1996), and where deliberations based on feedback are witnessed by neutral observers who are in turn able to help revise or modify the

original decisions. This happens less with decisions made by the military; but, per Smallman (2012), by possibly reducing mistakes, military decision-making would improve were this information available before decisions are made.

Along the lines proposed by Freer and Perdue that strongly defended arguments best provide justice, Lewis and Baker (2014) reach a somewhat similar conclusion that intellectual property (IP) strongly defended against cybercrime best protects national security:

> We know that balanced IP protection incentivizes growth. This is why nations have, for 150 years, put in place agreements to protect IP. Weak IP protections reduce growth and [encourage] IP theft over the Internet by increasing the scale of theft to unparalleled proportions; this both lowers and distorts global economic growth.

Good Cyber Defender Characteristics From the perspective of cognitive science, good cyber defenders require tools to support situation awareness. Good defenders are those made aware of the threats against them through better education, training and modeling (e.g., leadership). From the perspective of interdependence theory, in that cyber defense is a critical mission task, good cyber defenders should contribute to the multitasking actions of an organization in a way that optimally contributes to a teams' mission, including teamwork for cyber defense.

9.7.7 Summary

Cyber security is not a single, discrete, static entity. It is a dynamic system of hardware, software and people that experiences continuous change. Modeling cyber security threats becomes extremely hard, unless we take human factors into account and we begin to account for the decision-making processes of attackers and defenders. The kinds of research needed for this system demand a convergence of analyses among the domains of computer science, cognition, information science, mathematics, and networks in natural and social settings. For example, when modeling adversarial intent with respect to planning, proliferating, and potentially using cyber-attacks, researchers must utilize methods ranging across analytical, computational, numerical, and experimental topics to integrate knowledge useful for multi-disciplines, to improve the rapid processing of intelligence, and to rapidly disseminate action information to users.

Other Challenges To achieve many of the goals we have already discussed, fundamental challenges exist in the cognitive and information cyber-attack sciences:

- Researchers need to explore the attributes of complex, often independent computer and social networks; to explore related motivations for cyber-attacks; and to explore the decision factors used to defend these networks.
- Researchers need a better understanding and prediction of individual and group dynamics associated with the acquisition, proliferation and potential use of cyber-attacks, especially for massive attacks and of the behavior and vulnerabilities of physical and social networks underlying these dynamics.

- Researchers need to develop methods and techniques in response to the challenges of big data to better understand the factors influencing network robustness, dynamics, and concepts of operation, and how the defensive decisions that are made interdependently affect the strategic decisions of adversaries.

Having this cyber knowledge will significantly enhance the situational awareness of cyber-threats. To gain this knowledge, several research directions can be identified and organized into the following categories:

1. Cyber Pre-Attack (e.g., modeling motivation, "mind infections", dark-webs, defensive techniques, and interactions between groups);
2. Cyber Post-Attack (e.g., minimizing impacts of an attack, modeling and preventing cascading failures; providing tools that support understanding of interactions between networks and network elements);
3. Dynamical Interdependent Networks (i.e., networks that function by interacting; e.g., transportation; power); and
4. Computational Capability (e.g., to meet big data challenges; these challenges can be static or dynamic and linear or nonlinear).

In addition, we have identified and listed below known research gaps:

1. Real data is needed to validate models of both networks and cyber motivations, threats, attacks and mitigations;
2. Optimization metrics and the prioritization to select among them are needed;
3. Techniques are needed to incorporate geometric and temporal dynamics for both data collection and responses; and,
4. New models are needed to study human network interactions.

To fill the first gap, collaborations to obtain the sources of data and methods along with cross-testable results are needed for an archive that enables subject matter experts and others from different disciplines to study the archive. For the second gap, interactions are required between network owners and users on the one hand and academics, industry and government on the other to allow a meaningful search for the crucial metrics of cyber-defense performance. The third gap, in temporal dynamics, is currently being addressed from many different angles. The fourth gap, human and network interactions, represents a new area of research that must justify additional resources needed to fund wide-ranging collaborations among researchers across multidisciplinary areas that include computers, cognition, information, mathematics, and networks in natural and social sciences.

9.8 Conclusions

We draw a few conclusions from our review along with a brief discussion.

First, the cyber environment is becoming more and more complex along with the threats affecting cyberspace. For example, "By 2020 Cisco estimates that 99 % of devices (50 billion) will be connected to the Internet. In contrast, currently only

around 1 % is connected today." [32] Even defenses are becoming complex, whether a defense is passive or active (e.g., despite our lengthy review of cyber defenses, we omitted numerous defenses, such as the use of encrypting emails, randomly generating passwords,[33] using peer networks to increase security[34], hardening websites, etc.). One of the problems with defending a website against cyber threats is that the relative value of what is being protected increases to cyber-attackers as the defenses they face increase, fueling the arms race between cyber hackers and cyber defenders (Schwartz 2014).

This chapter review is not inclusive of all potential cyber threats. We omitted many threats, such as those for businesses that must handle private personnel information (Washington Post 2014, 6/23).[35]

> But unlike Settles's other [business] experiments . . . [with Obamacare] he is still trying to figure some things out—for example, how to safeguard employee information that must now be reported to the Internal Revenue Service, such as the Social Security numbers of children who are covered under their parents' health plans. "We don't want to be liable for that," he said. "What if we get hacked?"

Second, time criticality may be important. Actions can occur at wire speed in cyber, but 'slow and low' attacks like APTs are very difficult to detect and often sit until pre-specified conditions are met. A metric to watch is the cost of the defensive decisions per unit of time per unit of defense resource (from Walters 2014). The implication is that too much cost for cyber defense leads some businesses to settle instead of to defend (i.e., the example we used above where "ransomware" is used by cybercriminals to encrypt a firm's proprietary information and then seeking a fee to decrypt exemplifies the cost of a failed strategy; New York Times 2014, 6/21). Instead of settling, businesses and others must be persuaded that a better strategy is possible with improved defenses (Wall Street Journal 2014, 6/30).

Third, APTs are becoming a larger threat to national defense. For example, Naji (2004), Zarqawi's Islamist strategist "proposed a campaign of constant harassment of Muslim states that exhausted the states' will to resist." (see also The New Yorker 2014, 6/17) Harassment is apparently a characteristic of cyber-attacks against businesses such as when the attackers hold computer assets hostage until their ransom demands are met.

---

[32] e.g., http://communities.intel.com/community/itpeernetwork/blog/2014/02/08/cyber-security-is-not-prepared-for-the-growth-of-internet-connected-devices.

[33] http://csrc.nist.gov/publications/fips/fips181/fips181.txt.

[34] e.g., https://communities.intel.com/community/itpeernetwork/blog/2014/02/13/intel-cyber-security-briefing-trends-challenges-and-leadership-opportunities-cyberstrat14.

[35] See also: "The health care info that was hacked (and bank account info) may have affected contractors as well as both former and current employees. Their names, addresses, birth dates, Social Security numbers and dates of service were also included in the mix." From the *Wall Street Journal* (2014, 6/26), "Montana Breach Affects Up To 1.3 Million As Health Care Data Gets Hacked", http://www.wallstreetotc.com/montana-breach-affects-1-3-million-health-care-data-gets-hacked/24807/.

Fourth, a list of open cognitive science questions was noted that need to be addressed. For example, we need to know, based on cognitive science, the characteristics of good cyber defenders. We need to know the biases of attackers, users and user groups. We also need to explore the steps that can be taken to counter biases to better defend users from cyber-attackers.

Fifth, questions exist also for the interdependence in teams, organizations and systems. From interdependence theory, we need to know how to make teams into better cyber defenders; e.g., based on theory, maintaining the boundaries of good teams should generate less entropy—the evidence, supporting our hypothesis, indicates that the best teams generate less noise, but this evidence is anecdotal (Lawless et al. 2013). We have also found that internally cooperative teams compete better in increasingly competitive environments.[36]

To further develop interdependence theory, we need to better understand the limits of teamwork as cooperation, competition, boundaries, training and technology interact in interdependent environments. We have found that in a competitive world, as teams cooperate to improve their competitiveness, a team's boundaries are strengthened and better maintained (Lawless et al. 2013).

Interdependence theory informs us that boundaries can be maintained by searching for organizational vulnerabilities. Using attacks by "red" teams (Wall Street Journal 2014, 4/28) to search the cyber defenses for vulnerabilities in "blue" teams aids in helping organizations to better defend against cyber-attacks (Schwartz 2014). We agree with Martinez (2014) that system predictions and assessments are currently weak or nonexistent; system defenses need to be practiced and improved and automated where possible (e.g., with AI); and metrics established, measured and reported. Even though we warned that predictions made under interdependent states are clouded by uncertainty, predictions must be made of expected system performance during cyber games, followed by assessments of the metrics for the systems that suffered from red attacks. Comparative analyses of all of the teams playing cyber games need to be assessed and compared against real systems affected by actual cyber-attacks. But, in addition, we want to understand how malicious agents select targets—not just watch them do it. We should be able to create a system that predicts a malicious action before a red team composed of humans enacts a threat. Based on data sets of past cyber threats and defensive actions, predictive cyber threat analytics that predict future threats should become a part of the tool kit used by defenders against malicious actors.

From an individual perspective, cognitive biases form individual vulnerabilities that cyber-attackers attempt to exploit. However, from an interdependent perspective, team training offsets these biases (Lawless et al. 2013). The more competitive is a team, the more able it is to control its biases or limit the extent of their effectiveness

[36] Indirectly supporting our conclusion, HHS reported "... that more competition among health plans tends to lower prices ...", *Washington Post* (2014, 6/18), "Federal insurance exchange subsidies cut premiums by average of 76 %, HHS reports"; http://www.washingtonpost.com/national/health-science/federal-insurance-exchange-subsidies-cut-premiums-by-average-of-76percent-hhs-reports/2014/06/17/4f31b502-f650-11e3-a3a5-42be35962a52_story.html.

(e.g., as with varying levels of cyber defenses; as with checks and balances; in Lawless et al. 2013; or as with the use of "red" teams; in Schwartz 2014).

Finally, to optimize defenses against cyber-threats, we must shift our focus from an individual to the interdependent perspective. According to methodological individualism, cooperation produces the superior social good even if punishment is necessary to replace competition with cooperation (Axelrod 1984, p. 8). But, taken to its logical extreme justifies the savagery used by the Islamic State when it forces its people to be more cooperative (e.g., Naji 2004). Moreover, this theoretical perspective cannot wish away the threats and risks posed by cyber-attacks. In contrast, the realism of interdependence theory confirms that competition will remain ever present in the struggle for survival, driving the need for disruptive technology. From Kello (2013, p. 31):

> The revolutionary impact of technological change upsets this basic political framework of international society, whether because the transforming technology empowers unrecognized players with subversive motives and aims or because it deprives states of clear "if-then" assumptions necessary to conduct a restrained rivalry.

Competition and disruptive technology combine to create the very real present and future dangers we face in cyberspace; Again from Kello (2013, p. 32):

> The cyber domain is a perfect breeding ground for political disorder and strategic instability. Six factors contribute to instrumental instability: offense dominance, attribution difficulties, technological volatility, poor strategic depth, and escalatory ambiguity. Another—the "large-N" problem—carries with it fundamental instability as well.

Staying ahead in the race for new technology is important. In the future, Martinez (2014, p. 8) foresees two things for cyber defenders, that tying speech to visual data needs to be improved (e.g., vocal interactions with recommender displays); and that:

> The development of the recommender system . . . is an area of future research applicable to a broad range of applications, including . . . cyber anomaly detection . . . Such an approach will incorporate multiple disciplines in data aggregation, machine learning techniques, augmented cognition models, and probabilistic estimates in reaching the shortest decision time within the courses of action function of a decision support system.

Awareness is increasing of the dangers in cyberspace to Americans and the need to prepare to face those dangers. Recently in the *Wall Street Journal*, Tom Kean and Lee Hamilton (Kean and Hamilton 2014), the former chair and vice chair of the 9/11 Commission, respectively, and now co-chairs of the Bipartisan Policy Center's Homeland Security Project, spoke to these dangers:

> A growing chorus of national-security experts describes the cyber realm as the battlefield of the future. American life is becoming ever more dependent on the Internet. At the same time, government and private computer networks in the U.S. are under relentless cyber-attack. This is more than an academic concern—attacks in the digital world can inflict serious damage in the physical world. Hackers can threaten the control systems of critical facilities like dams, water-treatment plants and the power grid. A hacker able to remotely control a dam, pumping station or oil pipeline could unleash large-scale devastation. As terrorist organizations such as the Islamic State grow and become more sophisticated, the threat of cyber-attack increases as well.

To remain competitive and in business, organizations must be able to defend the proprietary information that they oversee for themselves and their customers in cyberspace (Finch 2014):

> The real game change for many CIOs [Chief Information Officer] is the emerging movement to consider a company's cybersecurity posture when making procurement decisions. To put it bluntly, companies with weaker cybersecurity are increasingly being viewed as less attractive vendors. . . . Already companies that have suffered successful cyber-attacks are finding themselves cut off from revenue streams. Just ask USIS, which performs background investigations for the U.S. government. USIS recently suffered a serious data breach, resulting in the personal information of tens of thousands of government employees being compromised. The response from its federal customers, the Department of Homeland Security and the Office of Personnel and Management, was swift: it was issued "stop-work" orders. And "stop-work" means no money coming in from either DHS or OPM. Worse yet, OPM announced earlier this week that it was not renewing its background check contract with USIS.

References

Abramson, M, (2014), Learning Temporal User Profiles of Web Browsing Behavior, Proceedings of the 6th ASE Conference on Social Computing.

Abramson, M. & Aha D. W. (2013), Authentication from Web Browsing Behavior, FLAIRS Conference.

Adelson, E. H. (2000). Lightness perceptions and lightness illusions. The new cognitive sciences, 2nd Ed. M. Gazzaniga. MIT Press.

Ahdieh, R.G. (2009), Beyond individualism and economics, retrieved 12/5/09 from ssrn.com/abstract=1518836.

Ambrose, S.H. (2001), Paleolithic technology and human evolution, Science, 291, 1748–53.

Axelrod, R. (1984). The evolution of cooperation. New York, Basic.

Axelrod, R. & Iliev, R. (2014), Timing of cyber conflict, PNAS, 111(4): 1–6.

Bell, B. S., Kozlowski, S.W.J. & Blawath, S. (2012). Team Learning: A Theoretical Integration and Review. The Oxford Handbook of Organizational Psychology. Steve W. J. Kozlowski (Ed.). New York, Oxford Library of Psychology. Volume 1.

Bernard, M. & Backus, G. (2009), Modeling the Interaction Between Leaders and Society During Conflict Situations, Sandia National Laboratories; Presented to the System Dynamics Society, Boston; see at: http://www.systemdynamics.org/conferences/2009/proceed/papers/P1382.pdf

Boebert, E. (2010), A survey of challenges in attribution, Proceedings of a workshop on deterring cyberattacks.

Capelle, Q. (2014, 1/24), "Multiple device users insufficiently aware of risks", from http://www.atelier.net/en/trends/articles/multiple-device-users-insufficiently-aware-risks_427025

Carley Kathleen M., et al. (2013), Liu, H., Pfeffer, J., Morstatter, F. & Goolsby, R. "Near real time assessment of social media using geo-temporal network analytics." Advances in Social Networks Analysis and Mining (ASONAM), IEEE/ACM International Conference on. Niagara, ON, Canada, August 25–29, 2013.

Chakrabarti, C.G. & Ghosh, K. (2013), Dynamical entropy via entropy of non-random matrices: Application to stability and complexity in modeling ecosystems, *Mathematical Biosciences*, 245: 278–281.

Darwin, C. (1973) The descent of man. New York, Appleton.

Feldman, J.M. & Lynch, Jr., J.G. (1988), Self-Generated Validity and Other Effects of Measurement on Belief, Attitude, Intention, and Behavior, Journal of Applied Psychology, Journal of Applied Psychology, 73(3): 421–435.

Finch, B.E. (2014, 9/11), CIOs Spur Revenue Generation Through Smart Cybersecurity, the *Wall Street Journal*, http://blogs.wsj.com/cio/2014/09/11/cios-spur-revenue-generation-through-smart-cybersecurity/?KEYWORDS=cyber+threats

Forsythe, C., Silva, A., Stevens-Adams, S.M. & Bradshaw, J. (2012), Human Dimensions in Cyber Operations Research and Development Priorities, SANDIA REPORT, SAND 2012–9188, http://www.jeffreymbradshaw.net/publications/Hum%20Dim%20Cyber%20Workshop%20Final%20Report.pdf

Fox News (2010, 3/8), "FBI Warns Brewing Cyberwar May Have Same Impact as 'Well-Placed Bomb'", from http://www.foxnews.com/tech/2010/03/08/cyberwar-brewing-china-hunts-wests-intel-secrets/

Freer, R. D. & Perdue, W.C. (1996), Civil procedure, Cincinatti: Anderson.

Giles, L. (2007), The art of war by Sun Tzu, Special Edition Books

Hackman, J. R. (2011). "Six common misperceptions about teamwork." Harvard Business Review blogs.hbr.org/cs/

Hartmann, K. & Steup, C. (2013), "The Vulnerability of UAVs to Cyber Attacks—An Approach to the Risk Assessment", in K. Podins, J. Stinessen & M. Maybaum (Eds.), 5th International Conference on Cyber Conflict, NATO CCD COE Publications

Kahneman, D. (2011), "Thinking fast and slow", MacMillan.

Kaplan, S. & Garrick, B.J. (1981), On The Quantitative Definition of Risk, Risk Analysis, 1(1): 11–27.

Kean, T. & Hamilton, L. (2014, 9/10), "A New Threat Grows Amid Shades of 9/11. The nation remains largely unaware of the potential for disaster from cyberattacks", Wall Street Journal, from http://online.wsj.com/articles/tom-kean-and-lee-hamilton-a-new-threat-grows-amid-shades-of-9-11-1410390195

Kelley, H.H. (1992), "Lewin, situations, and interdependence." Journal of Social Issues 47: 211–233.

Kello, L. (2013), "The Meaning of the Cyber Revolution. Perils to Theory and Statecraft", International Security, 38(2): 7–40.

Kenny, D. A., Kashy, D.A., & Bolger, N. (1998). Data analyses in social psychology. Handbook of Social Psychology. D. T. Gilbert, Fiske, S.T. & Lindzey, G. Boston, MA, McGraw-Hill. 4th Ed., Vol. 1: pp. 233–65.

Lawless, W. F., Llinas, James, Mittu, Ranjeev, Sofge, Don, Sibley, Ciara, Coyne, Joseph, & Russell, Stephen (2013). "Robust Intelligence (RI) under uncertainty: Mathematical and conceptual foundations of autonomous hybrid (human-machine-robot) teams, organizations and systems." Structure & Dynamics 6(2).

Lawless, W.F., Mittu, R., Jones, R., Sibley, C. & Coyne, J. (2014, 5/20), "Assessing human teams operating virtual teams: FIST2FAC", paper presented at HFE TAG 68, Aberdeen Proving Ground, May 20–22, 2014.

Lewis, M. (2014), Flash boys: a wall-street revolt. New York: Penguin.

Lewis, J.A. & Baker, S. (2014, June), "Net Losses: Estimating the Global Cost of Cybercrime. Economic impact of cybercrime II," Center for Strategic and International Studies. http://csis.org/files/attachments/rp-economic-impact-cybercrime2.pdf

Los Angeles Times (2014, 6/10), "FAA for the first time OKs commercial drone flights over land". http://www.latimes.com/business/aerospace/la-fi-faa-bp-drone-20140609-story.html

Loukas, G., Gan, D. & Vuong, T. (2013, 3/22), A taxonomy of cyber attack and defence mechanisms for emergency management, 2013, Third International Workshop on Pervasive Networks for Emergency Management, IEEE, San Diego.

Lowrance, W.W. (1976), Of acceptable risk: science and the determination of safety, Kaufmann Publisher.

Mallery, John C. (2011), "Models of Escalation in Cyber Conflict," presentation at the Workshop on Cyber Security and Global Affairs, Budapest, May 31–June 2, 2011, retrieved from http://es.slideshare.net/zsmav/models-of-escalation-and-deescalation-in-cyber-conflict.

Marble, J. (2014, 5/1), "Cognitive science for cybersecurity". Unpublished slides.

Martinez, D., Lincoln Laboratory, Massachusetts Institute of Technology (2014, invited presentation), Architecture for Machine Learning Techniques to Enable Augmented Cognition in the Context of Decision Support Systems. Invited paper for presentation at HCI.

McMorrow, D. (2010), "The Science of Cyber-Security,", Mitre Corp. report JSR-10–102, requested by JASON, retrieved from http://www.fas.org/irp/agency/dod/jason/cyber.pdf

Naji, A.B. (2004), The management of savagery. http://azelin.files.wordpress.com/2010/08/abu-bakr-naji-the-management-of-savagery-the-most-critical-stage-through-which-the-umma-will-pass.pdf

National Research Council of the National Academies (2012), "Terrorism and the Electric Power Delivery System" Washington, D.C.: National Academies Press, p. 16.

New York Times (2014, 6/20), "Hackers Take Down World Cup Site in Brazil"; from http://bits.blogs.nytimes.com/2014/06/20/hackers-take-down-world-cup-site-in-brazil/?_php=true&_type=blogs&_r=0

New York Times (2014, 6/21), "Hacker Tactic: Holding Data Hostage. Hackers Find New Ways to Breach Computer Security".

NIST's Special Publication 800–122 (2010, April), "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII);" from http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

NIST (2014, 2/12), "NIST Releases Cybersecurity Framework Version 1.0", http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm

Okhravi, H., Haines, J.W. & Ingols, K. (2011), "Achieving cyber survivability in a contested environment using a cyber moving target", *High Frontier Journal*, 7(3): 9–13.

Pfeffer, J., & Fong, C.T. (2005). "Building organization theory from first principles: The self-enhancement motive and understanding power and influence." Org. Science **16**: 372–388.

Pomerantsev, P. (2014, 5/5), "How Putin Is Reinventing Warfare", Foreign Policy, http://www.foreignpolicy.com/articles/2014/05/05/how_putin_is_reinventing_warfare.

Pressé, S., Ghosh, K., Lee, J. & Dill, K.A. (2013), Principles of maximum entropy and maximum caliber in statistical physics, Reviews of Modern Physics, 85: 1115: 1141.

Glowniak J (1998), "History, structure, and function of the Internet; Semin Nucl Med., 28(2):135–44; from http://www.ncbi.nlm.nih.gov/pubmed/9579415

Rajivan, P., Champion, M., Cooke, N.J., Jariwala, S., Dube, G & Buchanan, V. (2013), Effects of teamwork versus group work on signal detection in cyber defense teams. Lecture Notes in Computer Science, 8027: 172–180. P

Rand, D.G. & Nowak, M.A. (2013), Human cooperation, *Cognitive Sciences*, *17*(8): 413–425.

Reason, J. (2008), The Human Contribution, Unsafe Acts, Accidents and Heroic Recoveries, University of Manchester, UK: Ashgate.

Salim, H. (2014), "Cyber safety: A systems thinking and systems theory approach to managing cyber security risks". Working Paper CISL#2014–07, Sloan School of Management, MIT.

Schwartz, C. (2014, 6/10), "Program overview/challenges"; presentation to the 2014 Computational methods for decision making gathering, Arlington, VA, 10–12 June 2014.

Schweitzer, F., Fagiolo, G., Sornette, D., Vega-Redondo, F., Vespignani, A., & White, D.R. (2009). "Economic networks: The new challenges." Science **325**: 422–425.

Smallman, H. S. (2012). TAG (Team Assessment Grid): A Coordinating Representation for submarine contact management. SBIR Phase II Contract #: N00014–12-C-0389, ONR Command Decision Making 6.1–6.2 Program Review.

Smith, W. K., & Tushman, M.L. (2005) "Managing strategic contradictions: A top management model for managing innovation streams." Organizational Science **16(5)**: 522–536.

The New Yorker (2014, 6/17), "ISIS's savage strategy in Iraq; www.newyorker.com/online/blogs/comment/2014/06/isis-savage-strategy-in-iraq.html

Thibaut, J.W., & Kelley, H.H., (1959). The social psychology of groups. New York: Wiley.

USA Today (2014, 6/4), "Russian hacker engineered dazzling worldwide crime spree".

Valukas, A.R. (2014, 5/29), “Report to Board of Directors of General Motors Company Regarding Ignition Switch Recalls”; Published by *The Washington Post*. http://www.scribd.com/doc/228338387/Valukas-Report-on-GM-Redacted

Wall Street Journal (2009, 4/8), “Electricity Grid in U.S. Penetrated By Spies”, http://www.wsj.com/articles/SB123914805204099085

Wall Street Journal (2014, 4/28), “Europe Begins Its Largest-Ever Cyberwar Stress Test”; http://blogs.wsj.com/digits/2014/04/28/europe-begins-its-largest-ever-cyberwar-stress-test/?KEYWORDS=cyber+threat

Wall Street Journal (2014, 6/30), “Cyber Specter Mandates New CFO-IT Dynamic;” from http://deloitte.wsj.com/riskandcompliance/2014/06/30/cyber-specter-mandates-new-cfo-it-dynamic/?KEYWORDS=cyber+threat

Walters, J.P. (2014, 6/12), “Heterogeneous cloud services”; presentation to the 2014 Computational methods for decision making gathering, Arlington, VA, 10–12 June 2014.

Washington Post (2011, 8/3), “Report on ‘Operation Shady RAT’ identifies widespread cyber-spying“, from http://www.washingtonpost.com/national/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html

Washington Post (2014, 5/30), “China’s cyber-generals are reinventing the art of war”, http://www.washingtonpost.com/blogs/innovations/wp/2014/05/30/chinas-cyber-generals-are-reinventing-the-art-of-war/

Washington Post (2014, 6/6), “Vodafone reveals that governments are collecting personal data without limits. Britain’s Vodaphone cites several nations [29 nations are cited in its 88 page annex]. Warns that governments have unfettered access”, http://www.washingtonpost.com/business/technology/governments-collecting-personal-data-without-limit-says-vodafone/2014/06/06/ff0cfc1a-edb4-11e3-9b2d-114aded544be_story.html.

Washington Post 2014, 6/12), “FCC unveils ‘new regulatory paradigm’ for defeating hackers”, http://www.washingtonpost.com/blogs/the-switch/wp/2014/06/12/fcc-chair-telecom-companies-must-do-more-to-defend-against-hackers/

Washington Post (2014, 6/13), "P.F. Chang’s diners have card data stolen", http://www.washingtonpost.com/business/economy/pf-changs-diners-have-card-data-stolen-priceline-to-buy-opentable/2014/06/13/596ab6f4-f2a9-11e3-bf76-447a5df6411f_story.html

Washington Post (2014, 6/23), “As health-care law’s employer mandate nears, firms cut worker hours, struggle with logistics”, http://www.washingtonpost.com/national/health-science/as-health-care-lawles-employer-mandate-nears-firms-cut-worker-hours-struggle-with-logistics/2014/06/23/720e197c-f249-11e3-914c-1fbd0614e2d4_story.html

Wickens, C. D. (1992). Engineering psychology and human performance (second edition). Columbus, OH, Merrill.

Wired (2012, 11/09), “Teenage Hacker ‘Cosmo the God’ Sentenced by California Court”, retrieved from http://www.wired.com/2012/11/hacker-cosmo-the-god-sentenced-by-california-court/

Zipf, G.K. (1949), *Human behavior and the principle of least effort*, New York: Addison-Wesley.