

AMERICAN INTELLIGENCE JOURNAL

THE MAGAZINE FOR INTELLIGENCE PROFESSIONALS



Cyber Security and Operations

NMIA

2010

NMIA Board of Directors

LTG (USA, Ret) James A. Williams, Chairman, Board of Directors

Col (USAF, Ret) William Arnold, Director
LCDR (USCG) Michael E. Bennett, Advisor
MSgt (USAF, Ret) Thomas B. Brewer, Director
CAPT (USNR) Denny Brisley, Advisor
CDR (USNR, Ret) Calland Carnes, Director
Mr. Joseph Chioda, PMP, Director
Mr. Antonio Delgado, Jr., Vice President
MG (USA, Ret) Barbara G. Fast, Director
Lt Gen (USAF, Ret) Lincoln D. Faurer, Director
COL (USA, Ret) Michael Ferguson, Director
Col (USAF, Ret) Donna Fore, Director
Dr. Forrest R. Frank, Secretary-Treasurer
Col (USAFR, Ret) Michael Grebb, Director

COL (USA, Ret) Charles J. Green, Director
COL (USA, Ret) David Hale, Director
COL (USA, Ret) William Halpin, Director
LTG (USA, Ret) Patrick M. Hughes, Director
Mr. Pierre Joly, Director
Col (USAF, Ret) Joe Keefe, President
MG (USARNG) Edward Leacock, Advisor
RADM (USN, Ret) Rose LeVitre, Director
Mr. Mark Lovingood, Director
Mr. Gary McDonough, Director
Mr. Jon McIntosh, Director
Mr. Cornelius F. O'Leary, Director
LTG (USA, Ret) Harry E. Soyster, Director

Editor - COL (USA, Ret) William C. Spracher, Ed.D.

Associate Editor - Mr. Kel B. McClanahan, Esq.

Editor Emeritus - Dr. Anthony D. McIvor

Production Manager - Ms. Debra Hamby-Davis

The *American Intelligence Journal* (AIJ) is published by the National Military Intelligence Association (NMIA), a non-profit, non-political, professional association supporting American intelligence professionals and the U.S. Intelligence Community, primarily through educational means. The Board of Directors is headed by Lieutenant General James A. Williams (USA, Ret), and the president of NMIA is Colonel Joe Keefe (USAF, Ret). NMIA membership includes active duty, former military, and civil service intelligence personnel and U.S. citizens in industry, academia, or other civil pursuits who are interested in being informed on aspects of intelligence. For a membership application, see the back page of this *Journal*.

Authors interested in submitting an article to the *Journal* are encouraged to send an inquiry – with a short abstract of the text – to the Editor by e-mail at <William.Spracher@dia.mil>. Articles and inquiries may also be submitted in hard copy to Editor, c/o NMIA, 256 Morris Creek Road, Cullen, Virginia 23934. Comments, suggestions, and observations on the editorial content of the *Journal* are also welcome. Questions concerning subscriptions, advertising, and distribution should be directed to the Production Manager at <Admin@nmia.org>.

The *American Intelligence Journal* is published semi-annually. Each issue runs about 100 pages and is distributed to key Government officials, members of Congress and their staffs, and university professors and libraries, as well as to NMIA members, *Journal* subscribers, and contributors. Contributors include Intelligence Community leaders and professionals as well as academicians and others with interesting and informative perspectives. Back issues of the *AIJ* are available to members within the U.S. at the cost of \$25; to non-members and international requestors at \$50.

Copyright NMIA. Reprint and copying by permission only.

N
M
I
A

C
O
R
P
O
R
A
T
E

M
E
M
B
E
R
S

Accenture
Advanced Technical Intelligence Center
American Military University
American Systems Corporation
ANSER, Analytic Services, Inc.
Battelle Memorial Institute
BOSH Global Services
CACI
Computer Sciences Corporation
Concurrent Technologies Corporation
DynCorp International
DynCorp-Phoenix Training Center
General Dynamics Advanced Information Systems
Harding Security Associates, Inc.
Henley-Putnam University
JB&A, Inc.
KMS Solutions, LLC
L-3 Communications
LexisNexis Advanced Government Solutions
Lockheed Martin, IS&GS, Global Security Solutions
Northrop Grumman Corporation
Pluribus International Corporation
Riverside Research Institute
Science Applications International Corporation (SAIC)
SOS International, Ltd.
Sytera, LLC
TAD PGS
Textron Systems
USGC, Inc.
Zel Technologies, LLC

Table of Contents

President's Message	1
Editor's Desk	2
Cyber Death in Cyber Time and Cyber Space by Paul Milton Hobart	5
Cybersecurity: A Primer by CDR Peter J.B. Gottlieb	18
Treasure Trove or Trouble: Cyber-Enabled Intelligence and International Politics by Dr. Chris Bronk	26
Hallways and Doors: Deception in Cyberspace by Jason R. Weiss.	31
China's First War in the Global Era: Leadership Signaling in the Sino-Vietnam War by Timothy R. Heath	37
Chairman of NMIA Board of Directors Saluted in Support of Scholarships for Intelligence Studies by Dr. William C. Spracher	42
Getting to El Dorado Canyon: The Reagan Administration's 1986 Decision to Bomb Libya by Michael Moss	45
Teaching Intelligence Analysis with TIACRITIS by Dr. Georghe Tecuci, Dr. David Schum, Dr. Mihai Boicu, Dr. Dorin Marcu, Dr. Benjamin Hamilton, and Benjamin F. Wible	50
Chinese Corporate Espionage by Gary Sibeck	66
Kinetic Targeting of U.S. Citizens in the War on Terror: A Legal and Policy Perspective by Capt (USAF) Eric McCutchen	72

The opinions expressed in these articles are those of the authors alone. They do not reflect the official position of the U.S. government, nor of the National Military Intelligence Association, nor those of the organizations where the authors are employed.

AMERICAN INTELLIGENCE JOURNAL

Table of Contents (*Continued*)

In My View...

- Intelligence Oversight: Street Fight or Delicate Dance?
by COL (USAR, Ret) William H. Drohan 83

Profiles in Intelligence series...

- Liberazione d'Italia: One Woman's War
by Luis Carlos Montalvan 87

The Role of Austro-Hungarian Intelligence in World War I

- Andreas Figl: World War I Austrian Codebreaker
by Dr. Kenneth J. Campbell 94

- Maximilian Ronge: Master Spy
by Dr. Kenneth J. Campbell 100

NMIA Bookshelf...

- Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence*
reviewed by LTC (USA) Anthony Shaffer 109

- Treachery: Betrayals, Blunders, and Cover-ups: Six Decades of Espionage Against America
and Great Britain*
reviewed by Erik D. Jens 111

- U.S. National Security, Intelligence, and Democracy: From the Church Committee to the
War on Terror*
reviewed by Charles Carey 113

- Intelligence for an Age of Terror*
reviewed by MAJ (USA) Douglas W. Zimmerman 114

The opinions expressed in these articles are those of the authors alone. They do not reflect the official position of the U.S. government, nor of the National Military Intelligence Association, nor those of the organizations where the authors are employed.

Cybersecurity: A Primer

by CDR Peter J.B. Gottlieb

The national security of the United States, our economic prosperity, and the daily functioning of our government are dependent on a dynamic public and private information infrastructure, which includes telecommunications, computer networks and systems, and the information residing within. This critical infrastructure is severely threatened.

This cyber domain is exponentially expanding our ability to create and share knowledge, but it is also enabling those who would steal, corrupt, harm or destroy the public and private assets vital to our national interests. The recent intrusions reported by Google are a stark reminder of the importance of these cyber assets, and a wake-up call to those who have not taken this problem seriously. Companies who promptly report cyber intrusions to government authorities greatly help us to understand and address the range of cyber threats that face us all.

Dennis C. Blair, then-U.S.
Director of National Intelligence (2010)¹

It seems that everything relies on computers and the Internet now—communication (email, cell phones), entertainment (digital cable, mp3s), transportation (car engine systems, airplane navigation), shopping (online stores, credit cards), medicine (equipment, medical records), and the list goes on. How much of your daily life relies on computers? How much of your personal information is stored either on your own computer or on someone else's system?

Cyber security involves protecting that information by preventing, detecting, and responding to attacks.

US CERT (2010)²

Cyberspace is becoming a mirror image of the real world but without normal physical constraints and rules as time, space, and perimeters, enabling traditional and new actors to meet and interact with nearly the speed of light, thus making traditional thinking with

regard to protection obsolete and hugely challenging. The state's information and communication technology (ICT³) could be perceived as the central nervous system in an organism, or perhaps even a global nervous system,⁴ to comprehend its function and vulnerability. Interconnected and interdependent systems controlled and driven increasingly by digital technology are the backbones of many developed states. This trend, also known as *convergence*, makes it hard to predict and analyze the precise damage by coincidental or intended damage. The borderline between cyberspace and infrastructure is blurred⁵ and furthermore a lot of this infrastructure is privately owned and commercially driven, as stated by President Obama: "The vast majority of our critical information infrastructure in the United States is owned and operated by the private sector."⁶ Thus, most developed states are dependent upon private sector service in order to carry out their functions of state internally and externally. Connectivity is the ability to access the Internet and utilize online resources, and typically a high percentage of these are in developed states.

Cyber security is not simply about keeping systems accessible, but equally about authenticity, confidentiality, accessibility and integrity. During the last decade, there has been a shift from prestige-driven attacks to profit and politically driven attacks,⁷ along with increasingly sophisticated techniques. One of the challenges is to identify who is behind the actions, known as the attribution problem. Some non-state actors might use cyberspace to influence the security of the state, as this might affect the overall perception of the population. Normally, state security connects to domains where states have a central position, where cyberspace has to be understood in its own terms. As RAND states: "Cyberattacks, for instance, are enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities."⁸ The United States of America, Australia, and the United Kingdom have issued their intended plans and actions – the U.S. as a White House Policy Review⁹ and Australia¹⁰ and UK¹¹ as national cyber strategies. Both NATO¹² and the EU¹³ are also developing strategies and capabilities to counter the threat from cyberspace. In common they all focus on illegal actions in cyberspace, but they are not as focused on

the legal use of cyberspace with a hostile intent (e.g. spreading of ideology, support to that ideology, and funding and recruitment of new members.

The legal use of cyberspace in the information-driven conflict, utilizing the free flow of information in cyberspace, causes a dilemma that might challenge the security of the state. As Barry Buzan states: "Since governments largely determine the international activity and orientations of states, and since changes in governments, even for purely domestic reason, can result in significant shifts in international behavior, it is no surprise that states interfere in each other's domestic politics."¹⁴ Here is a connection to influence the nation-state's internal coherence and legitimacy through strategic communications, where different adversaries beside states might achieve strategic effect using cyberspace as a weapon or media, also known as cyber influence.¹⁵ David Kilcullen points out that we have to organize for this new challenge, as traditional sectorial fragmentation of resources and responsibility is inadequate to cope with the threat evolution.

We need an interagency effort, with leadership from the very top in the executive and legislative branches of government, to create capabilities, organizations, and doctrine for a national-level strategic information campaign. Building such a capability is perhaps the most important of our many capability challenges in this new era of information-driven conflict.

David Kilcullen (2007)¹⁶

The point of departure for this article is a description of cyberspace threats and dynamics in a holistic perspective, trying to make a complex issue and domain more tangible. Consequently, the article will focus on cyberspace as domain and not so much the influence upon the cognitive domain mentioned in regard to strategic communication. This article will sort motives by four objectives: authenticity, confidentiality, accessibility, and integrity, and subsequently extract possible actors.

CYBERSPACE AS DOMAIN

Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies (ICT).

Daniel T. Kuehl (2009)¹⁷

This chapter will investigate the threat where cyberspace is both the medium and the tool for hostile/unlawful actions and where different actors strive to get the upper hand in cyberspace. Well-known examples are the attacks on Estonia in 2007 and Georgia in 2008, with the attack on Estonia reflecting political pressure and coercion.¹⁸ The attack on Georgia was supporting a conventional attack. The most important feature of the attack was the blocking of information from inside Georgia to the outside world.¹⁹

Derived from the above-mentioned definition of cyberspace, it appears critical to determine how much is actually a part of, or connected to, cyberspace. In developed countries, ICT supports information exchange between humans, humans to systems, systems to human, and between technical systems. This underlines how widespread the use of ICT is, and why we are so dependent upon a reliable and resilient cyberspace. Four objectives are highlighted in this article, as they encompass both the defenders' and attackers' objectives. This will facilitate the understanding of cyberspace as a battlespace, and why different actors might have the same objectives, but differ in capabilities and motivation.

INTEGRITY

- Information must remain unchanged during storage and transport.
- Are the data/information trustworthy?

CONFIDENTIALITY

- Unauthorized personnel may not gain access to the information.
- Could unauthorized persons have had access to the data/information?

ACCESSIBILITY

- System must be stable and not break down.
- Is the system/network available on demand?

AUTHENTICITY

- The receiver must know that the sender is who he/she/it claims to be.
- Is the sender the person/system that can be immediately identified?

The fulfillment of these four objectives means that cyberspace can be used with efficiency, security, and confidence; if one or more are not obtained the entire perception and utilization will be affected negatively. Described mathematically, the product of these four objectives should not equal zero, and thus one objective must not equal to zero. This applies to all forms of utilizing cyberspace as a medium for communication, data

exchange, and support to ICT infrastructure as an essential contribution to the critical infrastructure. At the same time, these objectives should also specify exactly what the opponent wants to achieve, but which may be of the opposite value. The objectives have the strength that they can be used in relation to both defense and threat. The UK defines critical infrastructure as comprising key elements in nine sectors, which deliver essential services: energy, food, water, transport, communications, government and public services, emergency services, health, and finance.²⁰ The objectives emphasize the important role of confidence in using ICT, as the confidence in critical infrastructure depends upon ICT. There are other reasons for damage to cyberspace such as fire, lack of maintenance, incompetence, and natural disaster, which might inflict damage in varying degrees. The damaging effects might be as severe as the intended and hostile actions, but these are not within the scope of this article.

THE CYBER TOOLBOX

In order to conduct a cyber attack one needs two kinds of capabilities: analytical and technical. The analytical capability is necessary to identify the critical nodes and vulnerabilities, and the technical capability is to understand computers and networks. A way to label an adversary's capabilities is on a scale from *simple* to *complex*:²¹

Simple cyber attacks could be carried out by anyone (individual) with basic skills. No special resources or organizational structures are needed. Typically this type of attack focuses on a single target, e.g., defacement (takeover of, or editing, a website). These kinds of attacks are extremely common on the Internet today.

Potential use: harassment.

Advanced cyber attacks differ from simple attacks as the attacker (individual to small team) has the ability to write programs or to modify those of others, and also has a working knowledge of networks, operating systems, and possibly even defensive techniques (skills equal those of a Microsoft Certified Systems Engineer). This kind of attack typically focuses on a single type of system or network, i.e., a single organization or several using similar technologies.

Potential use: tactical attacks

Complex cyber attacks are significantly more difficult to accomplish. They require a team of individuals (or multiple teams) in a number of areas, including but not limited to networks, operating systems, programming languages, infrastructure technologies and control systems

(SCADA),²² intelligence gathering, and analysis and planning. Multiple targets with the coordination of multiple attack vectors require a sophisticated test bed, which is expensive. This kind of attack is often presented as a most likely scenario in the media and movies, but reality does not support this in numerical terms.

Potential use: strategic attacks.

The logic threat aims at the ICT-systems, where cyberspace is the medium from which the attacker launches his attack or utilizes cyberspace to achieve his goals. The tools mentioned below show some of the possibilities at hand for the adversary, but as cyberspace evolves in non-linear ways, the same goes for malware. It is not possible to attach specific tools to specific adversaries; only the sophistication in techniques might differ and give a hint of resources behind the development.

INTEGRITY

Information/data must remain unchanged during storage and transmission.

- Some viruses have a characteristic that alters or deletes data randomly on the victim's computer/system.
- Editing of audiovisual data is a special discipline where sound and video clips might be changed. Consequently, the trustworthiness of the originator is maintained alongside the new message. Defacement of websites is one kind of attack, where the attacker changes the content.
- A Trojan is a piece of malware that typically enters the computer via an attached file or by visiting infected sites specially designed for the purpose.

CONFIDENTIALITY

Unauthorized persons must not be allowed access to information/data.

- ARP poisoning²³ will give a local hacker the possibility to tap phones using Voice over Internet Protocol (VoIP) and disclose confidential information as passwords and log-on profiles.
- Sniffers are malware designed to be placed in the router, where it might intercept the traffic passing by and transmit this information to the attacker.

- Some worms transmit random information from the victim's computer to random contacts inside the mail program. Other worms switch on the victim's webcam, and transmit the pictures to the attacker.
- A key logger is a piece of malware that records all typing upon the victim's keyboard. The key logger program transmits the data to the attacker when the computer is online.
- Identity theft is an attacker obtaining access to personal data, e.g., social security information, driver's license, credit card information, etc. This will make the attacker able to pretend to be the victim in money transactions and e-commerce, or perhaps in social hacking (defined under "Authenticity" below).

ACCESSIBILITY

The systems must be stable and robust, and not liable to being forced to shut down.

- Viruses have been developed that make changes in the computer's settings, causing the computer to destroy vital hardware/software, sometimes making it unoperational.
- Worms in some cases lock the computer/server, or even destroy it, making it inaccessible.
- (Distributed) denial-of-service (D)DOS: servers and entire networks will be flooded with huge amounts of traffic, making them break down due to the huge masses of traffic. Usually hijacked computers (maybe even yours) are part of a botnet, used to attack infrastructure in another state or to send spam.

AUTHENTICITY

The receiver must be certain that the transmitter is who he/she/it pretends to be.

- Social hacking occurs between humans when, for example, the attacker might present himself as another employee, e.g., from the help desk, and insist that he needs the log-on and password immediately in order to perform some crucial operations.
- (Spear) phishing and Pharming are new and more severe threats. Here, users are lured into certain sites, which will install malware on the victim's computer. This will allow the attacker to steal the e-

identity or economic information, making him able to transfer the victim's money to other accounts.

- ARP poisoning will give a local hacker (insider on local network) the potential to pretend to be another person, and might obtain confidential information in that manner, e.g., phone tapping, passwords, etc.

An upcoming threat is supply chain attack where malware concealed in hardware parts is added during manufacturing. Today's complex networks and computer systems are typically a combination of parts from many subcontractors, where the last in the chain do not have control of each and every single part. Depending on the malware, all of the above parameters could be targeted. This type of attack might easily get inside secure and air-gapped networks, based on an Internet protocol. Because it is cheaper to make standard software (commercial off the shelf-COTS) operate separated from the Internet, the standard software is typically separated from the Internet by crypto or air gap.²⁴ However, when malware penetrates through this barrier it will operate with the same effectiveness as on the Internet.

Actors in cyberspace. A way to categorize the motives behind the actors is by the three Ps:

PRESTIGE, PROFIT AND POLITICAL

Of course, it is not possible to distinguish between these categories with absolute clarity, as more than one might influence one specific action. These categories serve the purpose of distinguishing between the different actors, and at the same time making a prediction regarding their capability and purpose. What makes threat evaluation difficult is the ease by which the actors might disguise themselves, and the possibility of merging into the huge amount of traffic. The adversaries which pose a strategic threat in this article are:

Foreign states have the resources to build a highly sophisticated capability and develop the technology and analysis needed. On this basis, they are the most threatening actor. As states want to be able to deny participation in an attack, they might choose to carry out their actions by a proxy hacker establishment in order to create deniability in the event of disclosure.²⁵ For the time being, it seems cyber espionage is the area of effort. The Internet is a gift to the intelligence community, as the reach is global with nearly the speed of light and with a good chance of success combined with little chance of disclosure. At the same time, there is evidence that several states are building an offensive capability in cyberspace,²⁶ which

could indicate a more traditional balancing mechanism between states.

Nation-states are primarily driven by political motivation and in some cases profit if industrial espionage gives the state a competitive advantage. As James A. Lewis, a national security expert at the Center for Strategic and International Studies said with regard to the Google-China incident in January 2010:²⁷ “This is a big espionage program aimed at getting high-tech information and politically sensitive information – the high-tech information to jump-start China’s economy and the political information to ensure the survival of the regime... This is what China’s leadership is after. This reflects China’s national priorities.” This illustrates the duality in effort, where one objective is profit, another political. It is not merely China that is conducting cyber warfare, but also Russia, North Korea, Iran, Israel, France, the United States, and the United Kingdom that are widely known to possess state-of-the-art cyber espionage know-how used for economic and military intelligence gathering.²⁸

NATO defines the military capability in cyberspace as computer networked operations (CNO), consisting of computer network attack (CNA), computer network exploitation (CNE), and computer network defense (CND).²⁹ CNO focuses on support to military operations, where CNO might be one tool in the campaign’s toolbox. James A. Lewis also estimates that “serious cyber attack independent of some large conflict is unlikely. To transpose cyber to the physical world, there are remarkably few instances of a nation engaging in covert sabotage attack against another nation (particularly larger powers) unless they were seeking to provoke or if conflict was imminent.³⁰” More likely, serious cyber attacks could be used for retaliation or when *in extremis*. The London-based International Institute for Strategic Studies supports this view by stating that cyber warfare could become a decisive weapon of choice in future conflict between states.³¹

Terrorist organizations/non-state actors are primarily driven by political motivation and in some cases profit if they focus on fund raising. For most terrorist organizations, cyber attacks are less desirable compared to physical attacks, as the physical attacks attract more publicity and spread more terror. Terrorist organizations use cyberspace to communicate and coordinate within their organization or network for financial transactions, strategic communication, and the recruiting of new members.³² Intelligence gathering is also of relevance when planning physical attacks since the technology and analytical capabilities are available at small cost. Combined with a global presence in cyberspace and its anonymous character, this makes it an ideal strategic asset. Thus, cyberspace serves primarily two purposes to terrorist organizations:

internal and external communications and intelligence gathering. Terrorist organizations will not be able to launch complex cyber attacks in the near future,³³ but a few might be able to outsource or insource an advanced capability. If terrorist organizations in the future acquire the capacity to carry out complex attacks, physical attacks could be less desirable.

(International/transnational) criminal organizations are utilizing the Internet for coordination of activities in the real world, money laundering, blackmail, trafficking, and coordination of other activities and cyber crime. Transnational criminal gangs have evolved into businesslike organizations with a need for transnational communication and coordination, which is why cyberspace is the obvious choice.³⁴ Among the wide range of activities performed by these criminals in cyberspace the following should be highlighted: cyber fraud, cyber extortion, and money laundering. All of these might have severe implications for bigger companies and individuals with high-profile jobs in industry and government.³⁵ Online fraud generated 52 billion worldwide in 2007,³⁶ which illustrates the extent of the problem. Criminal organizations are primarily motivated by profit and are therefore dependent upon the infrastructure, and will only perform political actions when paid. For instance, Israel suspects Hamas or Hezbollah to have hired Russian cybercriminals for an attack against its networks.³⁷ Some cyber criminals (hackers) are very skilled and will be able to launch advanced to complex attacks, especially if a government backs them with resources.³⁸

Hackers (cyber criminals – script kiddies) cover a spectrum from a curious teenager who tries with less sophisticated tools to professionals who see themselves as a kind of freedom fighter for anarchistic ideologies to veritable cyber criminals with an economic motivation. The latter typically work in networks where they exchange and sell the stolen information and control of servers and home computers (known as botnets). Therefore, the last group is the most dangerous because they have both the will and capacity to carry out advanced to complex attacks. IBM estimated in 1998 that about 9% of hackers (in 1998³⁹: 100,000 hackers) were working with the targeted industrial espionage, while somewhere between 0.1 and 1% were terrorist-related. They are not necessarily the same hackers, as some work on a laborer basis. The remaining 90% of the hackers worldwide, the so-called “script kiddies,” are often young computer freaks that do not necessarily have economic interests, but are more driven by prestige.⁴⁰ For example, they may be high school students in Potomac who hacked into computers and perhaps changed their grades.⁴¹

Employees/insiders pose a severe vulnerability, because it is difficult to detect normal work routines from harmful actions. At the same time, this is difficult to counter, because it will degrade effectiveness if one should impose strict control and tight procedures on one's employees. Some insiders work as traditional agents and might represent actors from the other groups of actors. Some are employees who use their legitimate access to data and systems to steal information for personal gain or to destroy or edit data as an act of revenge. In addition, there will be an opportunity to harm the company/institution by sending messages in the company's official name, which probably will inflict damage to the company's image. It not possible to indicate precisely what motivates the insiders, as they might act as agents serving a higher cause or they might be driven by personal reasons, such as profit or revenge for

being bypassed for promotion or being dismissed. One example is the employee in a French bank who defrauded 7 billion U.S. dollars by manipulating the bank's trading systems.⁴² Another example is the employee and blogger inside Whitehall, who revealed observations from high-level political meetings including not so flattering observations of the Prime Minister, causing intense interest by the public and consequently traffic on the blog.⁴³ The blogger was never identified in spite of an investigation.

SUMMARY

This matrix summarizes links between objectives, motivation, and actors:

	Integrity	Confidentiality	Accessibility	Authenticity
Political	<p>Foreign states</p> <ul style="list-style-type: none"> - CNA to change data/information in critical infrastructure (e.g. economy, energy, information, health, etc.). <p>Terrorist org.</p> <ul style="list-style-type: none"> - Subversion, e.g. editing official communications. <p>Hackers</p> <ul style="list-style-type: none"> - Freelance for terrorist or foreign states. - Freedom fighters for ideologies (hacktivism). <p>Insider (agent)</p> <ul style="list-style-type: none"> - Might represent the above mentioned or other political objectives. 	<p>Foreign states</p> <ul style="list-style-type: none"> - Cyber espionage to obtain politically and strategic information. - CNE (e.g. prepare CNA). <p>Hackers</p> <ul style="list-style-type: none"> - Freelance for terrorists or foreign states. - Freedom fighters for ideologies (hacktivism). Disclosure of sensitive data to the public. <p>Terrorist org.</p> <ul style="list-style-type: none"> - Cyber espionage – prepare physical attack. <p>Insider (agent)</p> <ul style="list-style-type: none"> - Might represent the above mentioned or other political objectives. 	<p>Foreign states</p> <ul style="list-style-type: none"> - CNA (e.g. DDOS-attack, complex cyber attacks). - State censorship. <p>Hackers</p> <ul style="list-style-type: none"> - Freelance for terrorist or foreign states - freedom fighters for ideologies (hacktivism) <p>Terrorist org.</p> <ul style="list-style-type: none"> - DDOS in combination with physical terrorist attack. (advanced cyber attack). <p>Insider (agent)</p> <ul style="list-style-type: none"> - Might represent the above mentioned or other political objectives. 	<p>Foreign states</p> <ul style="list-style-type: none"> - Cyber espionage (social hacking) by luring humans into leaking information/data. - CNO (e.g., take-over of systems and networks). - Subversion. <p>Hackers</p> <ul style="list-style-type: none"> - Takeover of official website with own message. - Freedom fighters for ideologies (hacktivism). <p>Insider (agent)</p> <ul style="list-style-type: none"> - Might represent the above mentioned or other political objectives.
Profit	<p>Criminal org.</p> <ul style="list-style-type: none"> - Cyber fraud. <p>Hackers</p> <ul style="list-style-type: none"> - Freelance. <p>Terrorist org.</p> <ul style="list-style-type: none"> - Money transfer and fund raising. <p>Insider (employee)</p> <ul style="list-style-type: none"> - Fraud for personal gain. - Agent for competing company, foreign state, or organization. 	<p>Foreign states</p> <ul style="list-style-type: none"> - State-sponsored espionage to save the cost of research and development in state-owned companies. <p>Criminal org.</p> <ul style="list-style-type: none"> - Cyber extortion. Ransom for sensitive data, or disclosure. <p>Hackers</p> <ul style="list-style-type: none"> - Freelance for personal gain. <p>Insider (employee)</p> <ul style="list-style-type: none"> - Spying for competing company, foreign state. 	<p>Criminal org.</p> <ul style="list-style-type: none"> - Cyber extortion (both individuals and companies) where ransom must be paid to re-access data/systems. <p>Hackers</p> <ul style="list-style-type: none"> - Freelance for personal gain. <p>Insider (employee)</p> <ul style="list-style-type: none"> - Destroying a system/data for competing company, foreign state, or perhaps revenge. 	<p>Criminal org.</p> <ul style="list-style-type: none"> - Cyber fraud, e.g., phishing, credit card fraud, identity theft. <p>Hackers</p> <ul style="list-style-type: none"> - Freelance for terrorists or foreign states. <p>Terrorist org.</p> <ul style="list-style-type: none"> - Intelligence gathering (social hacking). <p>Insider (employee)</p> <ul style="list-style-type: none"> - Agent for competing company, foreign state (social hacking).⁴⁴
Prestige	<p>Hackers</p> <ul style="list-style-type: none"> - Script kiddies. - Ideology. <p>Insider (employee)</p> <ul style="list-style-type: none"> - Personal kick, e.g., altering data as revenge. 	<p>Hackers</p> <ul style="list-style-type: none"> - Script kiddies. - Ideology. <p>Insider (employee)</p> <ul style="list-style-type: none"> - Personal kick, e.g., disclosure of sensitive information. 	<p>Hackers</p> <ul style="list-style-type: none"> - Script kiddies. - Ideology. <p>Insider (employee)</p> <ul style="list-style-type: none"> - Personal kick, e.g., deleting data/ destroying systems as revenge. 	<p>Hackers</p> <ul style="list-style-type: none"> - Script kiddies. - Ideology. <p>Insider (employee)</p> <ul style="list-style-type: none"> - Revenge, make the company/authority look bad in public.

This matrix does not take likelihood and consequences into consideration. It is not possible to distinguish clearly between the different tools, as the same tools are available to all actors. What differs is the sophistication as mentioned under levels of attack, or the selection of tools being part of the concealment of identity. What becomes obvious is the blend of motives and actors, not similar to the way in which most states organize their defense. Most states organize their defense in sectors including both responsibility and resources. The attribution problem reinforces this situation, as some actors might act under a "false flag" in order to avoid disclosure, and thereby the possibility to be kept responsible for their actions.

As of now, cyberspace is still in an early stage of development and driven mostly by commercial interests. This is about to change as more and more states are becoming aware of their vulnerabilities; this is why they are developing security strategies and capabilities accordingly. The future will most likely introduce national and international rules, procurement standards, common security standards, and protocols that will decrease the

problems of attribution, education programs, and career paths regarding IT skills. In other words, they will be concerned with how to achieve the four objectives discussed in this article and at the same time deny those same objectives to any adversary.

Notes

¹Annual Threat Assessment of the U.S. Intelligence Community – Dennis C. Blair (2010-02-02).

² US CERT: <http://www.us-cert.gov/cas/tips/ST04-001.html>.

³ CSIS (2008) – Securing the cyberspace for the 44th presidency defines ICT as four critical sectors: "energy, finance, the converging information technology and communications sectors and government services (including state and municipal governments)," p. 44.

⁴ U.S. Department of State (2010). Speech by Secretary of State Hillary R. Clinton, "Remarks on Internet Freedom."

⁵ CSIS (2008) – Securing the cyberspace for the 44th presidency, p. 54 (SCADA and Industrial Control systems).

⁶ U.S. President Barack Obama (2009). Remarks by the President on securing the nation's cyber infrastructure.

⁷ *The Christian Science Monitor* (2010). "US oil industry hit by cyberattacks: Was China involved?"

CTC—Providing World-Class Services for World-Class Competitiveness



Concurrent
Technologies
Corporation

(800) CTC-4392 • www.ctc.com

- Advanced Distributed Learning
- Advanced Materials and Manufacturing Technologies
- C4ISR Systems
- Information and Network Systems Security
- Intelligence Analysis
- Modeling and Simulation
- State-of-the-Art Systems Design and Analysis
- Systems/Software Engineering
- Visualization

CTC is an Equal Opportunity Employer • M/V/D/F

⁸ RAND (2009). Project Air Force, p. III.

⁹ White House (2009) – Cyberspace Policy Review.

¹⁰ Australian Government (2009). Cyber Security Strategy.

¹¹ Cabinet Office (2009) – Cyber Security Strategy of the United Kingdom (June 2009).

¹² NATO Parliamentary Assembly (2010-01-06). NATO and Cyber Defense.

¹³ EU: Europe’s Information Society (2009).

¹⁴ Barry Buzan (1992). *People, States and Fear* (second edition), p. 88.

¹⁵ Cyberpower and National Security (2009), p. 343 (Chapter 14 by Franklin D. Kramer and Larry K. Wentz).

¹⁶ David Kilcullen (2007). *New Paradigms for 21st Century Conflict*.

¹⁷ Cyberpower and National Security (2009), p. 28 (Chapter 2 by Daniel T. Kuehl).

¹⁸ NATO (2007). Cyber attacks against Estonia in the spring of 2007.

¹⁹ McAfee
– Virtual Criminology Report 2009
– Virtually here: The Age of Cyber Warfare (2009), pp. 6-7.

²⁰ Cabinet Office (2009). National Cyber Security of the United Kingdom (2009), p. 9.

²¹ Cyberpower and National Security (2009), pp. 443-445 (Chapter 19 by Irving Lachow, paraphrased).

²² SCADA=Supervisory control and data acquisition, system monitoring and controlling, e.g., infrastructure systems or other large industrial complexes. SCADA often depends on information infrastructure (Internet) to operate or upgrade.

²³ Watchguard (2010) – Anatomy of an ARP Poisoning Attack.

²⁴ Air gap: when a system physically is kept offline.

²⁵ James Lewis (CSIS 2009). “The ‘Korean’ Cyber Attacks and Their Implications for Cyber Conflict,” p. 2.

²⁶ McAfee (2009) – Virtual Criminology Report 2009. p. 13.

²⁷ *The Washington Post* (2010). “Google China cyberattacks part of vast espionage campaign, experts say.”

²⁸ *USA Today* (2010). “China-Google quarrel highlights world of cyber espionage.” Quotation by Jody Westby.

²⁹ Mulvenon, James (2009), “PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability” pp. 257-259.

³⁰ James A. Lewis (CSIS 2009). The “Korean” cyber attacks and their implications for cyber conflict, p. 7.

³¹ *The Guardian* (2010). “Cyber-warfare ‘is growing threat’.”

³² Middle East Forum (2007). “The two faces of al-Qaeda.”

³³ Cyberpower and National Security, p. 450 (Chapter 19 by Irving Lachow).

³⁴ CNNMoney.com (2009). “Cybercrime: A secret underground economy.”

³⁵ *The Christian Science Monitor* (2010). “US oil industry hit by cyberattacks: Was China involved?”

³⁶ ACPO e-crime strategy version 1.0, p. 2 (2009).

³⁷ CSIS James Lewis (2009). “The ‘Korean’ Cyber Attacks and Their Implications for Cyber Conflict,” p. 8.

³⁸ Northrop Grumman (2009). “Capability of the People’s Republic of China to conduct cyber warfare and computer network exploitation,” pp. 41-45.

³⁹ This is quite old data, but newer statistics have not been available.

⁴⁰ Teletema no. 1 (1998).

⁴¹ *The Washington Post* (2010). “Students at Potomac school hack into computers; grades feared changed.”

⁴² BBC (2008), “Rogue trader to cost SocGen \$7bn.”

⁴³ *Times* online (2008). The hunt is on for the “Civil serf” demon blogger of Whitehall.

⁴⁴ Instead of breaking into a network, one fools the user to provide the correct log-on profile and password.

Commander Peter J.B. Gottlieb, Royal Danish Navy, is currently serving at the Royal Danish Defence College’s Institute for Strategy, where he analyzes the strategic challenges produced by cyberspace. He also supports the Senior Joint Staff Course as tutor and instructor. He served in the Danish fast patrol boat squadron, on fast attack crafts, and has performed staff duty within research and development activities at the Royal Danish Frogman Corps. Interested readers may contact him for more information at gottfader@yahoo.dk.



CDR Gottlieb presenting a lecture regarding strategic communication and its utilization in cyberspace at a seminar held by the Reserve Forces Association of Denmark.

