14/2

Volume 14 Number 2 • **Spring 2011**

IAnewsletter

The Newsletter for Information Assurance Technology Professionals

International Information Assurance

also inside

contents

About IATAC and the *IAnewsletter*
The *IAnewsletter* is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a Department of Defense (DoD) sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), and Assistant Secretary of Defense for Research & Engineering ASD(R&E).

Contents of the *IAnewsletter* are not necessarily the official views of or endorsed by the US Government, DoD, DTIC, or ASD(R&E). The mention of commercial products does not imply endorsement by DoD or ASD(R&E).

Inquiries about IATAC capabilities, products, and services may be addressed to—

IATAC Director: Gene Tyler
Inquiry Services: Ryan Skousen

If you are interested in contacting an author directly, please e-mail us at *iatac@dtic.mil.*

***IAnewsletter* Staff**
Chief Editor Gene Tyler
Assistant Editor Kristin Evans
Art Director: Tammy Black
Copy Editor: Barbara Veneri
Editorial Board: Al Arnold
Angela Orebaugh
Dr. Ronald Ritchey
Designers: Tammy Black
Lacey Olivares
Don Rowe

***IAnewsletter* Article Submissions**
To submit your articles, notices, programs, or ideas for future issues, please visit *http://iac.dtic.mil/iatac/IA_newsletter.html* and download an "Article Instructions" packet.

***IAnewsletter* Address Changes/Additions/Deletions**
To change, add, or delete your mailing or e-mail address (soft-copy receipt), please contact us at—

IATAC
Attn: Peggy O'Connor
13200 Woodland Park Road
Suite 6031
Herndon, VA 20171

Phone: 703/984-0775
Fax: 703/984-0773

E-mail: *iatac@dtic.mil*
URL: *http://iac.dtic.mil/iatac*

Deadlines for Future Issues
Summer 2011 May 6, 2011

Cover design: Tammy Black
Newsletter design: Donald Rowe

Distribution Statement A:
Approved for public release;
distribution is unlimited.

in every issue

IATAC Chat

Gene Tyler, IATAC Director

From time to time, we get questions at IATAC that are difficult to answer. Often the reason for the difficulty is that definitions evolve, and as they shift they re-enter a "development phase." Sometimes organizations do not agree on a single definition, and various organizations operate with different definitions. However, having clear, agreed upon definitions is important for organizations because definitions inherently identify missions, goals, objectives, and responsibilities.

The most recent example of questions that are difficult for IATAC to answer: What are the definitions of information assurance (IA) and cybersecurity? Are they the same or, if different, how so? Most agree that IA is defined as "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." This or very similar definitions are used in academia and industry. The functions described above evolved over time moving information security (INFOSEC) to what is now generally accepted as IA. Cybersecurity is evolving as many believe there is no firm definition yet and it might even include IA. I suspect that many organizations have an interest in this definition as the widely different roles of organizations might be adding to its flux. And we may not get one definition because various organizations have different needs and therefore view cybersecurity differently.

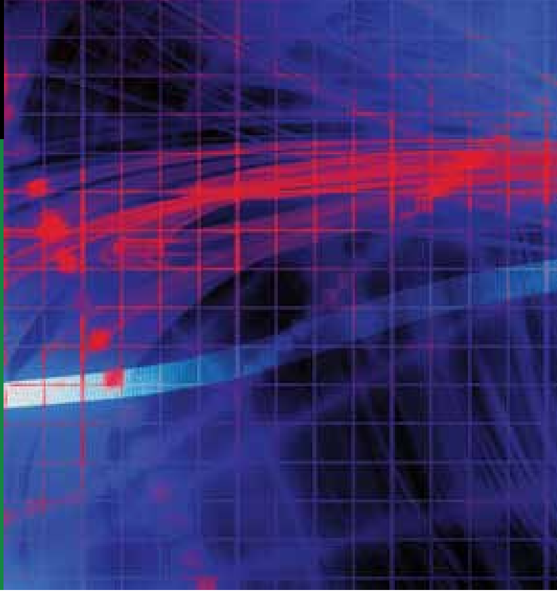
At the annual meeting with our executive steering committee members, IA leaders across the Department of Defense (DoD), representatives from the federal government and academia, this question came up. We have also been hearing from our subject matter experts (SMEs) and others as to what the definition of cybersecurity is and the comparisons between IA and cybersecurity. So we researched DoD and other federal government documentation; we asked our SMEs for their opinions; we interviewed IA and cybersecurity leaders in industry and from academic institutions; and researched open source materials. What did we find? There is a general, commonly-used definition for IA, but not a common, government and industry-wide definition for cybersecurity yet. As a matter of fact, we also found different spellings: *Cybersecurity, cybersecurity,* or *cyber security.*

So I ask you – our audience – what do you think? Please take a moment and send us your definition and source. I encourage you to go to the Armed with Science blog at *http://science.dodlive.mil* that IATAC posted in April and provide your comments and feedback – this will give you a way to respond and let others know your position. Of course, you are free to e-mail us at iatac@dtic.mil to provide feedback, also.

As always, this edition presents a host of interesting articles and an interesting mix of IA articles with an international flavor. Our featured SME and university are from the U.K., and we continue with an interesting article on NATO cyber defense exercises. This issue also highlights Rick Aldrich, IATAC's cyber law SME, who provides an interesting look at how and why international law is difficult to apply to cyber attacks. He discusses the difficulties in applying laws about traditional warfare to conflicts in cyberspace. This edition also includes articles about how information security and information sharing continue to improve. Chris Silva, our Ask the Expert columnist, provides an in-depth look into how organizations' information security practices will likely evolve over the next couple years. Brian Smith's article discusses how Move Beyond Green, a Web 2.0 site, facilitates information sharing and collaboration for the Army, helping to increase the long-term sustainability of the organization. We hope you can develop ideas for how to improve information security and information sharing from reading these articles.

In closing, I continue to ask for your thoughts and engagement. I am amazed at what we don't know, but we strive continually to gain more knowledge and our comparison of IA and cybersecurity (however it is spelled) reflects that point. I look forward to learning more about this important topic from you. Engage with us on our Armed with Science blog, or send a quick e-mail. What you think is important to us!!!

Gene Tyler



NATO Cyber Defense Exercises

by Kraig Cantwell

The North Atlantic Treaty Organization (NATO) works as an alliance of nations for the protection of all. In 2010, NATO established the Emerging Security Challenges Division (ESCD) to address many of the non-traditional security issues facing the alliance. One critical area is cyber defense. Suleyman Anil, the head of the Cyber division of ESCD, leads a team in developing cyber defense policies. Ambassador Gábor Iklódy, the assistant secretary general for ESCD, also chairs the Cyber Defense Management Board (CDMB), which is the primary governing body for recommending cyber defense guidance within the alliance. The CDMB, with the guidance of the NATO Consultation, Command and Control Board (NC3B) leads the team of NATO and national representatives who plan and execute annual cyber defense exercises. This Cyber Coalition brings together not only NATO nations, but also many other partner nations to train and develop capabilities necessary for defending critical information.

The diverse support that nations bring to operations, such as the International Security Assistance Force in Afghanistan, highlights the need to share time-critical information. Linking operational networks provides an effective way to enhance multinational operations. However, there are many risks. As the adage goes: "A risk within one nation is a risk shared by all."

NATO leadership realizes the need to establish sound cyber defense policies that can be executed by all nations.

As a result, NATO leadership realizes the need to establish sound cyber defense policies that can be executed by all nations. Trusting the security of one another's networks is vital to sharing information and means that every nation must dedicate the necessary resources to protect information systems. Nations must also work together to mitigate the risks that everyone faces to ensure the collective protection of shared information.

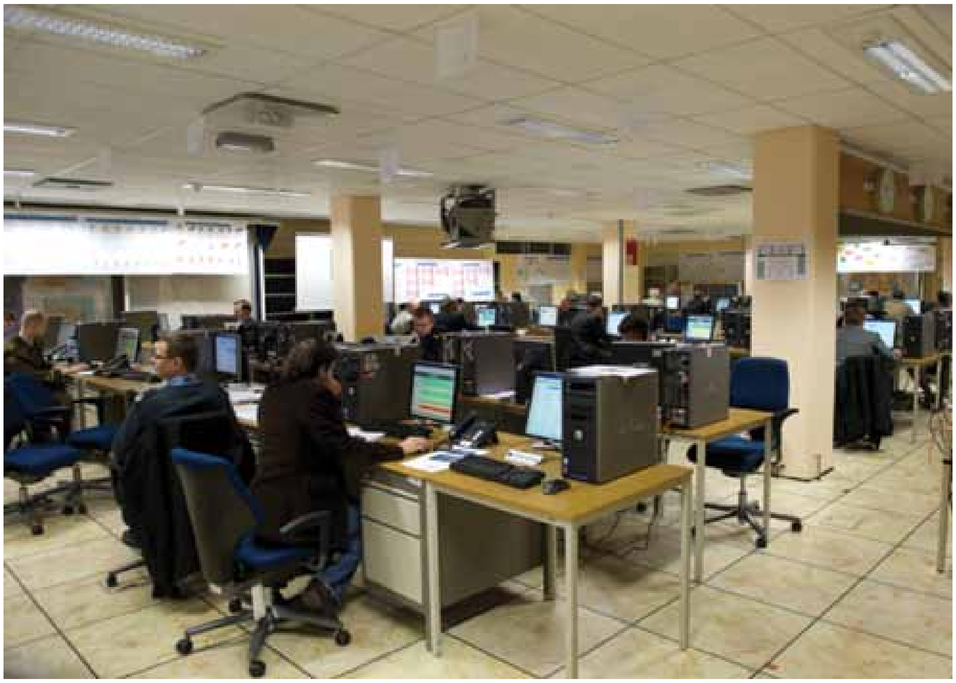


Figure 1 Cyber Coalition 2010, exercise control cell inside the bunker at SHAPE Headquarters, Mons, Belgium

Exercise, Cyber Coalition 2010 (CC10)

A few years ago, NATO leadership realized that to properly defend the alliance within the cyber domain, they would require trained staff, both technical and operational. The Cyber Coalition exercise series began in 2008, but was limited initially to only NATO organizations that exercised basic tactics, techniques, and procedures and refined and tested NATO cyber defense skills. The exercise proved to be a success, and CDMB leadership chose to expand participation in 2009 to include nine alliance nations that actively sought to participate. Many other alliance nations observed the exercise to determine how to participate actively in future years. In 2010, there were 13 alliance nations actively participating and 11 nations observing. Each year, the complexity of the exercise increases to ensure that staff members learn to deal with real-world cyber defense issues. A tentative goal for the 2011 exercise is to develop scenarios that allow all 28 NATO nations to participate in the exercise in some manner, along with numerous other non-NATO nations and international organizations.

The United States has participated throughout the planning and execution phases of the exercises to ensure NATO and the Department of Defense can get the maximum training possible. The Office of the Assistant Secretary of Defense, DoD, Chief Information Officer, Networks, Information and Integration (DOD-CIO/ASD (NII)) and the U.S. European Command (USEUCOM) have provided planning staff to assist the NATO core planners with scenario development. The USEUCOM cyber defense team, led by Col. Patricia Rinaldi, has actively participated during execution. They tested and validated new tactics, techniques, and procedures (TTPs) that were developed throughout the year. The U.S. Cyber Command (USCYBERCOM) assisted the USEUCOM exercise controller in Mons, Belgium, with one officer, who provided invaluable insight into how USCYBERCOM interacts with not only DoD leadership during times of crisis, but also with the U.S. Department of Homeland Security (DHS). The U.S. Computer Emergency Response Team from DHS also participated and provided valuable insight, especially during the initial phases, to develop TTPs for engagement with European nations' computer response centers

Figure 2 Deputy, Supreme Allied Commander Europe (DSACEUR) General Sir John McColl and NATO Assistant Secretary General for Emerging Security Challenges Ambassador Gábor Iklódy being briefed by Anna-Maria Talihärm from the core planning team

> Each year, training alliance members becomes increasingly important as operational networks are linked to enable and enhance information sharing.

operated by civilian organizations as well as military groups. This insight provided a lesson learned in the 2009 exercise, where problems with coordination between military and civilian organizations from different nations arose because of differing national policies.

The primary objectives for the 2010 exercises were to begin testing strategic decision making processes and to exercise the operational collaboration capabilities of NATO organizations and those of the participating nations. The 2010 exercises used tactical cyber defense scenarios to drive selected nations and NATO to collaborate and enable staff to coordinate defensive responses.

Each year, training alliance members become increasingly important as operational networks are linked to enable and enhance information sharing. Unclassified information sharing is a reality with the alliance, but sharing restricted or secret cyber defense information relevant to classified networks has proven more difficult. Many nations realize that not having international information sharing agreements in place has hindered information sharing efforts, especially in times of crisis. Another hurdle identified by the exercise presented itself when some nations engaged NATO using military cyber defense channels while other nations engaged with national organizations, resulting in a lack of information sharing because of policy constraints among nations.

These "lessons learned" have proven very useful in promoting nations to examine these problem areas, and many are now working to develop policies to facilitate rapid sharing of information. There were many other valuable lessons captured throughout the entire planning and execution of the exercise. These are being evaluated to ensure nations improve individually and as an alliance.

The Core Planning Team guides the team of planners from all the participating nations in developing the exercises. During the 2010 exercise, the planners developed numerous storylines for training staff across all aspects of NATO and participating nations. They worked closely with many nations who also linked their national cyber defense exercises to the NATO exercise. This enabled nations to provide greatly improved training because they could work the strategic processes fully within their nations before engaging with NATO.

Cyber Coalition 2010 attracted high level visibility in NATO circles. The Deputy Supreme Allied Commander Europe (DSACEUR) General Sir John McColl; the Director of NATO Communications and Information Systems Services Agency Lieutenant General Kurt Herrmann; and NATO Assistant Secretary General for Emerging Security Challenges Ambassador Gábor Iklódy visited the exercise coordination cell in Belgium during the execution of the exercise. They experienced firsthand how national controllers coordinate and collaborate to ensure success.

DSACEUR McColl commented: "I think it's remarkable how the exercise has developed this year. It has increased in scope and increased in ambition and I think that's entirely right and proper given the development of the threat."

Gen. Herrmann stated, "This is a most valuable event. We are using this not only for improving the procedures but also for training all personnel in the NATO Computer Incident Capability."

Ambassador Iklódy, the CDMB chairman, added: "The participants will reflect on what they will observe here and come back with some good ideas on how to improve our procedures. We will use those observations when developing NATO's Policy on cyber defense."

Planning for the Cyber Coalition 2011 exercise has already begun with the Core Planning Team meeting to develop scenarios for nations to review and comment on before the initial planning conference in April 2011. Anticipation is high that this next exercise can stimulate collaboration among nations and also enable nations to engage more effectively with NATO leadership on many more relevant aspects of cyber policy. For 2011, NATO leadership engagement can enable many more offices and organizations to participate actively in the exercises, enabling strategic decision-making processes to be exercised fully. NATO leadership encourages all NATO nations to participate in order to fully test the processes and procedures of the NATO cyber defense community. With many changes occurring in NATO cyber defense policies following the Lisbon Summit, the Cyber Coalition 2011 exercise should be an exciting event. ■

About the Author

Kraig Cantwell | currently supports the OSD(NII) as liaison to the European region for the International Information Assurance Program. He retired from the U.S. Air Force after serving for 22 years with a background in intelligence, operations, and communications. Kraig has been working information assurance and computer network defense programs in Europe for more than nine years. His current focus is on international engagement and information sharing among nations to ensure the defense of U.S. and partner nation information.

University of Greenwich

by Angela Orebaugh

The University of Greenwich is a British University with its main campus located in the borough of Greenwich in London, England. The university also includes two additional campuses in Avery Hill and Medway. The university includes nine schools and three institutes. The School of Computing and Mathematical Sciences (CMS) is an extremely successful part of the university and is recognized both nationally and internationally for its cutting edge research and its innovative approach to curriculum development.

CMS offers a wide range of degrees and specialist programs and consists of more than 100 academic and research staff. CMS offers the following advanced degrees focused on information assurance and security:

- **Computer Security Forensics and Risk Management**—This Masters of Science degree includes courses with topics such as computer crime and forensics, computer security and risk management, and network security. [1] This program has been designed around recognized international standards ISO 27001, ISO 9000-3 and BS 25999. It also closely follows the syllabi of the Certificate in Information Systems Auditing (CISA) and Certificate for Information Systems Security Professionals (CISSP) and provides a solid foundation for anyone wishing to gain these qualifications. [2]
- **Computer Forensics and Security Management**—This Masters of Science degree includes courses with topics such as computer crime, police and forensic methods, and the legal requirements for collecting evidence. At the end of the program, students can administer and configure business-critical distributed applications. They also gain an understanding of the threats to business networks and servers. The program includes hands-on training in current forensic tools used by the police (*e.g.*, EnCase, FTK, and WinHex). This program is accredited by the British Computer Society (BCS) and can lead to full exemption from the BCS postgraduate diploma and postgraduate diploma project. Additionally, this qualification awards partial chartered engineer (CEng) status and can be combined with a partial CEng from an accredited Bachelor of Science (BSc) course to give full CEng status.
- **Network and Computer Systems Security**—This Masters of Science degree covers software and hardware technologies, theoretical studies, and international standards and legal and regulatory requirements that pertain to computer security in different nations. The program also provides hands-on training in current industry-standard tools for implementing security (such as access control, authentication, encryption, and key management). Courses include topics such as operating system and application server security, risk management, and mobile technologies. This program is accredited by the BCS and can lead to full exemption from the BCS postgraduate diploma and corresponding project. Additionally, this qualification awards partial CEng status and can be combined with a partial CEng from an accredited BSc course to give full CEng status. [3] ■

References

1. *http://www.gre.ac.uk/courses/pg/com/compsec*
2. *http://www.gre.ac.uk/courses/pg/net/cfsm*
3. *http://www.gre.ac.uk/courses/pg/net/cnet*

Stuxnet Poses Interesting International Cyber Law Issues

by Rick Aldrich

Article 51 of the United Nations charter states in pertinent part, "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations." So can a cyber attack, such as that evidenced by Stuxnet, constitute an "armed attack?"

Stuxnet has been characterized by some as the most "advanced and aggressive malware in history," [1] and as a "warhead" [2] or "precision-guided cyber-munition" [3] by others. According to the latest information from Symantec, it checks for a very specific central processing unit (CPU) and a very specific communications module. [4] The Stuxnet malware also appears to check to ensure that the "industrial control system it has infected has frequency converter drives from at least one of two specific vendors, one headquartered in Finland and the other in Tehran, Iran."

Those frequency converters must be operating between 807 and 1210 Hz. Frequency converters operating in that range are export-regulated by the Nuclear Regulatory Commission since they can be used for uranium enrichment. If all the conditions are met, Stuxnet modifies the code of the target to adjust the output frequency to a much higher level and then a much lower level, ultimately sabotaging the target. Stuxnet's intended target appeared to be Iranian uranium enrichment facilities. Indeed, without naming Stuxnet directly, Iranian President Mahmoud Ahmadinejad admitted malicious software code had damaged Iran's centrifuge facilities.[5] An Institute for Science and International Security (ISIS) report suggested some 1,000 Iranian centrifuges at the Natanz facility may have been damaged by Stuxnet, basing their data on an analysis of International Atomic Energy Agency (IAEA) quarterly reports.[6]

"Natanz was built eight meters underground and was topped with dozens of meters of reinforced concrete and earth in 2004, in anticipation of a possible attack by Israeli or American 'bunker buster' bombs."[7] In spite of this, it appears Natanz was successfully and surreptitiously attacked by the malcode known as Stuxnet, without any loss of life and no response from the victim.

Some have suggested Israel was the perpetrator based on its special interest in preventing Iran from obtaining a nuclear weapon, the sophistication of the code, and various clues within it. Even more than a year and a half after it was discovered, however, there appear to be no conclusive links to the perpetrator. Let's analyze how international cyber law might address the Stuxnet incident.

Could Iran claim that Israel has perpetrated an "armed attack" against it, thereby permitting Iran to respond in self defense?

Armed Attack

Article 51 of the United Nations (UN) charter states in pertinent part, "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations." [8] So can a cyber attack, such as that evidenced by Stuxnet, constitute an "armed attack?"

Clearly at the time Article 51 was written, in August of 1945, such an attack was never envisioned. Traditionally the term “armed attack” has connoted a kinetic attack – missiles, bombs, bullets and the like – but it has never been definitively defined. Incidents like the cyber attacks against Estonia in 2007 and against Georgia in 2008 have prompted renewed interest in defining if or when a cyber attack can also constitute an “armed attack.” International legal scholars are increasingly moving away from the means of attack and instead looking to the effects. The test would be whether the effects of the attack are similar to those of a kinetic attack. Cyber attacks that result in physical damage, such as the destroyed centrifuges in the case of Stuxnet, may be pulled under the rubric of an armed attack, though this approach does not rule out attacks resulting in non-physical effects if the harm is substantial. Interestingly, in his testimony before the Senate Armed Services Committee, Lieutenant General Keith Alexander, then President Obama’s nominee to head the Defense Department’s new Cyber Command, suggested that the United States may employ self-defense even if it fails to meet the criteria of Article 51 when he stated: “If the President determines a cyber event does meet the threshold of a use of force/armed attack, he may determine that the activity is of such scope, duration, or intensity that it warrants exercising our right to self-defense and/or the initiation of hostilities as an appropriate response.”[9]

Traditionally the term “armed attack” has connoted a kinetic attack – missiles, bombs, bullets and the like – but it has never been definitively defined. Incidents like the cyber attacks against Estonia in 2007 and against Georgia in 2008 have prompted renewed interest in defining if or when a cyber attack can also constitute an “armed attack.”

Unlawful Use of Force

The “use of force” referenced in the above quotation is a reference to Article 2(4) of the UN charter, which states: “All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations.” [10] Some scholars have claimed that an unlawful use of force under Article 2(4) may not always rise to the level of an “armed attack” under Article 51, which permits a self-defense response. Even if Stuxnet were not deemed to constitute an armed attack, it may still be deemed an unlawful use of force, though there is a similar lack of consensus as to if and when a cyber attack may constitute an unlawful use of force. It is particularly muddled when the effect of the attack is merely to rearrange bits, such as modifying a database to falsely represent a logistical posture, interfere with banking transactions, or the like.

Threats to the Peace

Under Chapter VII of the UN charter, the Security Council is authorized to take certain actions, including employing armed force in response to “any threat to the peace, breach of the peace, or act of aggression.”[11] Each of these terms raises similar questions as to their interpretation with respect to cyber attacks.

Attribution

In the case of Stuxnet, the fact that approximately 10 percent of the centrifuges at one of Iran's most important uranium processing facilities were so physically damaged that they had to be replaced, resulting in a significant degradation to its energy and/or weapons production program, may well argue for pulling the incident under the ambit of Articles 2(4) and 51. But one would need to attribute the source of the attack, also. The language of Article 2(4) explicitly applies only to member states; so, unless the use of force is perpetrated by a nation-state, it is not within the ambit of the article. Article 51 does not have the same explicit restriction. In the wake of the attacks of September 11, 2001, the United States took self-defense actions against the terrorist organization Al Qaeda. Nevertheless, the attribution of the actor determines the legally appropriate response. If the cyber attack is the work of a 14-year old hacker, the response would be dramatically different from that which is appropriate against a nation-state sponsored attack. Individuals, criminal syndicates, and terrorists (notwithstanding the above counterexample) are generally subject to law enforcement actions.

> If Iran were somehow able to reliably attribute the source of the attack to a nation-state, what would Iran be permitted to do in self-defense? Generally, the Law of Armed Conflict requires that the response be both militarily necessary and proportionate.

This requirement to attribute the source of the attack proves to be one of the biggest hurdles in cyber attacks and is for Iran in responding to Stuxnet. While many have suggested the extreme sophistication of the Stuxnet malware suggests a state actor, others say that criminal and terrorist syndicates can produce highly sophisticated malware. Sophisticated cyber attacks often employ obfuscation and anonymization techniques to deter detection and traverse through multiple countries to make identification of the source legally challenging and time-consuming. Additionally, even if one identifies the source Internet Protocol (IP) address or addresses, one must also determine the controlling IP address (in the case of zombies, botnets, or other remotely controlled devices), the person behind the controlling IP, and the sponsor of that person (whether that be a nation-state, terrorist organization, criminal syndicate, or no sponsor). There is some indication that Stuxnet was delivered using removable media, either wittingly or unwittingly by someone with inside access. [12] This may make attributing the source even more difficult. Subtle clues in the malcode indicating that it may have been written by an Israeli have also been used to suggest it was done by a country trying to frame Israel, since some claim Israeli intelligence is too sophisticated to have left clues in the code that would point back to them.

> Interestingly, the United States in mid-2010 joined 14 other countries to pursue issues relating to a cyber arms control proposal…the group of countries "recommended that the U.N. create norms of accepted behavior in cyberspace, exchange information on national legislation and cybersecurity strategies, and strengthen the capacity of less-developed countries to protect their computer systems."

Cybercrime

If the attribution leads to an individual who cannot be reliably tied to a government sponsor, the individual could potentially be tried if Iran has criminal laws covering the conduct. The international Cybercrime Convention sets out a broad range of cybercrime laws that member states must enact through domestic legislation. [13] It also has provisions to facilitate attribution and extradition from one member state to another. Iran is not a member of the Cybercrime Convention, so it cannot avail itself of these provisions; but since the Stuxnet cyber attack resulted in physical damage to property, Iran may well want to try it under more general criminal laws and employ its existing extradition treaties, to the extent applicable.

Military Necessity and Proportionality

If Iran were somehow able to reliably attribute the source of the attack to a nation-state, what would Iran be permitted to do in self-defense? Generally, the Law of Armed Conflict requires that the response be both militarily necessary and proportionate. The concept of military necessity stipulates that targets must have a military goal and be consistent with the laws of war. The fact that military and civilian computer networks are often tightly intertwined and may serve multiple purposes may complicate matters. Even the highly sophisticated Stuxnet code appears to have been unable to confine itself to its apparently intended targets, ending up on more than 40,000 IP addresses in 155 countries. The concept of proportionality does not require the response be in-kind. That is, Iran would not be restricted to a cyber response, but would have to keep it comparable in scope. "The U.S. government, when they're dropping a bomb, they have all sorts of computer algorithms and studies that they use to show exactly what the consequences are going to be from dropping this bomb from this angle on this building, [but those] consequential analyses are much harder in cyberspace, and so it's hard to apply the proportionality test." [14]

Cyber Riots

If the victim had been a NATO country instead of Iran, would Stuxnet have triggered the collective self-defense provision of the NATO treaty? It is not clear, but the analysis would track proportionality as explained above because the collective self-defense provision of the NATO treaty is Article 5, and it uses the same "armed conflict" threshold and also links the provision directly to Article 51 of the UN charter. Interestingly, when Estonia, which is a NATO member, was the victim of a cyber attack in 2007 after it moved the Bronze Soldier of Tallinn, riling Russia and Russian nationalists, many characterized the attack as a "cyber riot," which suggests a civil disorder rather than an "armed attack;" and so NATO was never asked to provide support under Article 5.

Cyber Arms Control

Interestingly, the United States in mid-2010 joined 14 other countries to pursue issues relating to a cyber arms control proposal. The other countries include Belarus, Brazil, Britain, China, France, Germany, Estonia, India, Israel, Italy, Qatar, Russia, South Korea, and South Africa. The group of countries "recommended that the U.N. create norms of accepted behavior in cyberspace, exchange information on national legislation and cybersecurity strategies, and strengthen the capacity of less-developed countries to protect

> What constitutes an "armed attack," an "unlawful use of force," a "threat to the peace," "breach of the peace," or "act of aggression" in cyberspace is still far from clear, though an effects-based approach may provide a way beyond the traditional kinetic-based precedents.

their computer systems." [15] For many years, Russia has advocated a treaty that would ban military uses of cyberspace, but the United States has been reluctant to engage in such discussions because of the difficulty of attribution. With attribution still a stumbling block, and monitoring or controlling cyber "weapons" a significant challenge, it is unclear whether the legal regime of an international cyber arms control treaty could avert incidents such as Stuxnet in the future.

Another concern with cyber weapons is that, unlike most conventional and nuclear weapons which tend to self-destruct when used, cyber weapons can be captured, modified, and directed at new victims. Should countries that launch malware such as Stuxnet be required to take into account the collateral damage that may result when a target repurposes the weapon and re-releases it? Stuxnet was found on computers in some 155 countries around the world, even though about 60 percent of occurrences were in Iran. It did no harm in those hosts that did not meet all the criteria set out above, but what if actors at one of the infected sites manipulates the code slightly and re-releases it? Such tweaking could potentially permit the malware to attack a much larger group of Supervisory Control And Data Acquisition (SCADA) systems anywhere in the world.

International cyber attacks raise a myriad of issues under international law. This short article addressed only a few, but as evidenced even by these, cyber attacks do not fit cleanly within existing legal constructs. What constitutes an "armed attack," an "unlawful use of force," a "threat to the peace," "breach of the peace," or "act of aggression" in cyberspace is still far from clear, though an effects-based approach may provide a way beyond the traditional kinetic-based precedents. Attribution remains a significant stumbling block with no easy solution on the horizon. The concepts of military necessity and proportionality are harder to apply to cyber attacks and responses. Cyber arms control agreements may be an attempt to rein in this burgeoning problem, but can traditional inspection, verification, and compliance regimes work to control cyber weapons? [16] If not, the world needs to find an alternative. The security of our network-centric world may depend on it. ■

About the Author

Rick Aldrich | is the senior computer network operations policy analyst for IATAC. Previously, he served as the deputy staff judge advocate for the Air Force Office of Special Investigations, specializing in the cybercrime and information operations portfolios. He has been awarded several grants by the Institute for National Security Studies and has multiple publications related to the legal implications of information warfare. He has a B.S. in computer science from the U.S. Air Force Academy, a J.D. from UCLA, and an LL.M. in intellectual property law from the University of Houston.

References

1. Yaakov Katz, "Stuxnet virus set back Iran's nuclear program by 2 years," Jerusalem Post, Dec. 15, 2010 citing German computer consultant Ralph Langer (available at *http://www.jpost.com/IranianThreat/News/Article.aspx?id=199475).*
2. "Yet to turn; The Stuxnet worm," The Economist, Dec. 18, 2010.
3. "Hunting an Industrial-Strength Computer Virus Around the Globe," PBS Newshour, October 1, 2010 (available at *http://www.pbs.org/newshour/bb/science/july-dec10/computervirus_10-01.html).*
4. Information drawn from Nicolas Falliere, Liam O Murchu, and Eric Chie, "W32.Stuxnet Dossier," Symantec Security Response, version 1.3 (November 2010) (available at *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf).*
5. Mark Clayton, "Stuxnet: Ahmadinejad admits cyberweapon hit Iran nuclear program," Christian Science Monitor, Nov. 30, 2010 (available at *http://www.csmonitor.com/USA/2010/1130/Stuxnet-Ahmadinejad-admits-cyberweapon-hit-Iran-nuclear-program).*
6. *See* David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment," ISIS, Dec. 22, 2010 (available at *http://www.isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/).*
7. David Lev, "Stuxnet Virus 'Warheads' Could Knock Out Iran's Utility Systems," Israel National News, Nov. 24, 2010, citing Israeli security expert Rafael Sutnick (available at *http://www.israelnationalnews.com/News/News.aspx/140806).*
8. Article 51, United Nations Charter.
9. Responses to Senate Armed Services Committee Questions for Lieutenant General Keith Alexander, Nominee for Commander, United States Cyber Command, April 15, 2010, at 12.
10. Article 2(4), United Nations Charter.
11. Article 39, United Nations Charter.
12. "W32.Stuxnet Dossier," *supra* note 4.
13. The Cybercrime Convention, which has been signed by 47 nations and ratified by 30, including the United States, only addresses criminal activity by individuals, not nation-states.
14. Tom Gjelten, "Extending the Law of War to Cyberspace," National Public Radio, Sep. 22, 2010, quoting Harvard Law professor Jack Goldsmith (available at *http://www.npr.org/templates/story/story.php?storyId=130023318).*
15. Ellen Nakshima, "15 nations signal willingness to reduce cyberwarfare threat," Washington Post, July 17, 2010 at A2.
16. Paul Kerr, John Rollins, Catherine Theohary, "The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability," Congressional Research Service, Dec. 9, 2010 at 8.

DoDTechipedia Happenings

by Cheryl Bratten

Over the last few months, DoDTechipedia has made some exciting additions to the wiki. These changes help users organize information on DoDTechipedia, share opinions with a click of the mouse, and make it easier for you and your DoD colleagues to join the wiki.

DoDTechipedia's New Calendar Feature

One key element for effective collaboration includes coordinating dates and deadlines among members of a group.

On DoDTechipedia, you can add and edit a calendar on any page. This feature allows you to—

- Display one or multiple calendars with each calendar displayed in its own color
- Select day, week, and month views and choose the starting day for each week
- Link URLs or documents within specific events

You may ask how can a calendar help my group? Adding a calendar to a blog to highlight meetings and conferences or historical events important to your field is one way; creating a page for your project and adding a calendar for key project milestones or to link documents or URLs to the milestones is another; or you can add a calendar to your personal space to keep track of conferences you plan to attend in the coming months.

To add a calendar to any page in DoDTechipedia, click the *Edit* tab, then click *Wiki Markup*. Place the cursor where you want the calendar to display on the page; then input the code: {calendar:id=mycal|title=DTIC Calendar|firstDay=Sunday}. Add more calendars by clicking *Add a Calendar* in the right navigation pane of an existing calendar. After you click *Save*, the calendar is displayed, and you can begin adding information.

Share an Opinion with a Click of the Mouse

New to the DoDTechipedia wiki as of January 2011 is a polling feature. Every month, wiki organizers ask for your opinion on a topic of interest. You can find the question on the DoDTechipedia Welcome page. Select a response, and click *Submit* to register your opinion. After you vote, the responses of other DoDTechipedia users are displayed. Each poll remains active for two weeks.

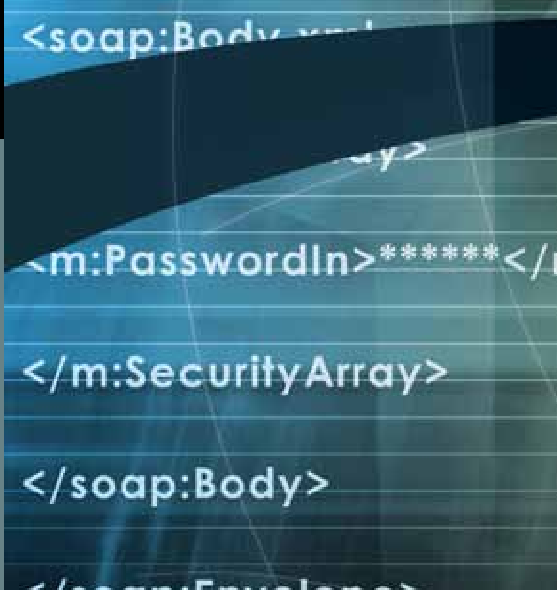
We also welcome feedback anytime through our online feedback form, "DoDTechipedia CARES." Visit *https://ca.dtic.mil/pubs/survey/FY11CARESDoDTech1.htm*, or click the DTIC CARES logo in the Customer Feedback section of the DoDTechipedia Welcome page, to provide feedback on improvements, problems, or to tell us how you use DoDTechipedia to accomplish your mission.

Registering for DoDTechipedia is Easy

Registering for access to DoDTechipedia is easy since the Defense Technical Information Center (DTIC) launched a new, streamlined registration process. Common Access Card (CAC) holders access DoDTechipedia with their CAC in the card reader; they are registered automatically for unclassified, limited information in DoDTechipedia, DTIC Online Access Controlled (DOAC), and Aristotle. To obtain access to classified or export-controlled information, follow the instructions in the Welcome e-mail to upgrade your account.

We have streamlined the process for non-CAC holders, too. DoD contractors without a CAC, federal employees, and contractors can fill out a shortened application. With our new registration process, now is the perfect time to invite colleagues to explore all that DTIC has to offer. To invite your colleagues to join DoDTechipedia, click the *Invite* drop-down menu on the top navigation bar, and click *Invite to Register*, or provide them the link to DOAC *(https://www.dtic.mil)*. ■

DoDTechipedia is a project of the Under Secretary of Defense for Acquisition, Technology and Logistics; Assistant Secretary of Defense for Research & Engineering; Defense Technical Information Center; and Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer.



Enhancing the Global Cyber Defense Workforce

by Johanna Vazzana

Six years before President Obama's recommendation, the Office of the Assistant Secretary of Defense for Networks and Information Integration/ Department of Defense CIO (ASD (NII)/ DoD CIO) began facilitating international cybersecurity partnering with the International Cyber Defense Workshop (ICDW). Introduced in 2003, the ICDW has grown from a face-to-face working group consisting of a handful of participants to its current state – a virtual web-based workforce development activity attended by nearly 300 participants from dozens of partner nations. The ICDW functions as an education and awareness activity for military cybersecurity practitioners, builds technical skills, and provides an opportunity for registrants to collaborate with global partners with the common purpose to advance the cyber workforce and minimize cyber threats.

Figure 1 President Obama has highlighted the need for increased cybersecurity

> "Only by working with international partners can the United States best address challenges, enhance cybersecurity, and reap the full benefits of the digital age."—2009 President's Cybersecurity Review

Since its inception, the ICDW has continuously grown and evolved, resulting in a series of "firsts." Beginning in 2003, ASD (NII)/DoD CIO partnered with the Information Technology and Operations Center (ITOC), a research center in the Department of Electrical Engineering and Computer Science at the United States Military Academy at West Point, N.Y. An initial workshop was designed to offer computer network defenders from the U.S., the United Kingdom, Canada, Australia, and New Zealand an opportunity to share capabilities and techniques in a collaborative, hands-on environment. In 2006, ASD (NII)/DoD CIO expanded the ICDW from an event in support of the specific objectives defined under the multilateral agreement with the United Kingdom, Canada, Australia, and New Zealand, to a workshop open to those partner nations that NII interacts with under the International Information Assurance Program (IIAP). One year later, the Royal Military College (RMC) became the first partner nation to host the workshop in Kingston, Ontario, Canada (Figure 2).

The year 2008 saw a significant growth point – the introduction of a completely virtual workshop. Using readily available open-source technology and virtual networks, participants could interact in real-time with instructors, other registrants, and workshop moderators using Defense Connect Online, a web-based application for training. Without the

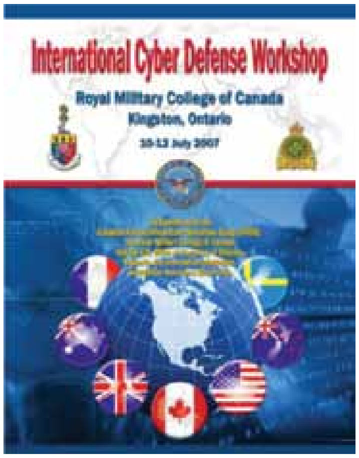

International Cyber Defense Workshop
Royal Military College of Canada
Kingston, Ontario
10-13 July 2007

Figure 2 First ICDW partner nation workshop

burden of travel expenses and time away from home offices, registration numbers skyrocketed. Because of increased international interest, the year 2009 brought the addition of a second workshop and an expanded list of partner nation invitations.

Today, ASD(NII)/DoD CIO extends invitations to more than 40 partner nations and defense organizations to participate in the ICDW, held twice a year in June and in November. With workshop sessions offered at multiple times around the clock, participants can enjoy the week-long workshop during their business day or during non-working hours regardless of their time zone. Cybersecurity professionals from academia, industry, and government act as virtual instructors, connecting to the workshop from their home stations around the globe. They deliver unclassified training and simulated attack-and-defend scenarios in the areas of computer network defense (CND), CND architecture, response and analysis, computing forensics, and threat mitigation. Workshop registrants use audio, video, and chat features to interact with instructors and with each other, making the workshop completely real-time and interactive. The Carnegie Mellon University Software Engineering Institute (SEI); the University of Nebraska, Omaha (UNO); McAfee, Inc.; and the Naval Postgraduate School contributed training and exercise components to the most recent ICDW in November 2010.

UNO has acted as technical leader for the workshop since 2008, providing registrants the opportunity for immediate, hands-on application of cybersecurity concepts with lab scenarios following each of the UNO-provided lectures. The UNO labs utilize System Administrator Simulation Trainer (SAST), a Government off-the-shelf (GOTS) toolkit developed by Pacific Northwest National Laboratory. SAST simulates a basic Internet environment, artificially generates network traffic, and superimposes real exploits on the simulated network.

Workshop registrants have also experienced Carnegie Mellon SEI's XNET platform, a virtual environment that allows small teams to collaborate and play a variety of roles such as attacker, defender, and controller. The Naval Postgraduate School, a newcomer to the ICDW, introduced the CyberCIEGE tool to more than 200 international registrants in November 2010. CyberCIEGE, an interactive game-like experience developed by the school's Center for Information Systems Security Studies and Research, allows registrants to immerse themselves in simulated situations that require risk analysis, followed by actions to both identify and configure the appropriate security controls to mitigate the risk.

Figure 3 First partner nation workshop

The ICDW currently attracts significant interest in the international cybersecurity domain and enjoys partnerships with Defense Cyber Crime Center (DC3), Department of Homeland Security (DHS), Defense Information Systems Agency (DISA), Defense-wide Information Assurance Program (DIAP), Pacific Northwest National Labs (Security Assessment Simulation Toolkit [SAST]), and the U.S. Marine Corps.

The next step for the ICDW is to create a virtual international cyber defense resources tool. Work is under way to expand an ICDW web portal, currently used for participant registration and administrative functions, to include information about pertinent cyber defense resources. Registrants for the June 2011 ICDW can enjoy the added benefit of information

▷▷ *continued on page 31*

SUBJECT MATTER EXPERT

Dimitrios Frangiskatos

by Angela Orebaugh

This article continues the profile series on members of the Information Assurance Technology Analysis Center (IATAC) Subject Matter Expert (SME) program. The SME profiled in this article is Dimitrios Frangiskatos of the University of Greenwich. Mr. Frangiskatos is a senior lecturer in the computer science department of the School of Computing and Mathematical Sciences. He is the 2010/2011 program leader for several information assurance degrees including—

- Master of Science (MSc) Computer Forensics and Security Management
- MSc Computer Systems and Network Engineering
- MSc Computer Forensics and Security Management
- MSc Computer Systems and Networking
- MSc Computer Forensics and Systems Security
- MSc Network and Computer Systems Security

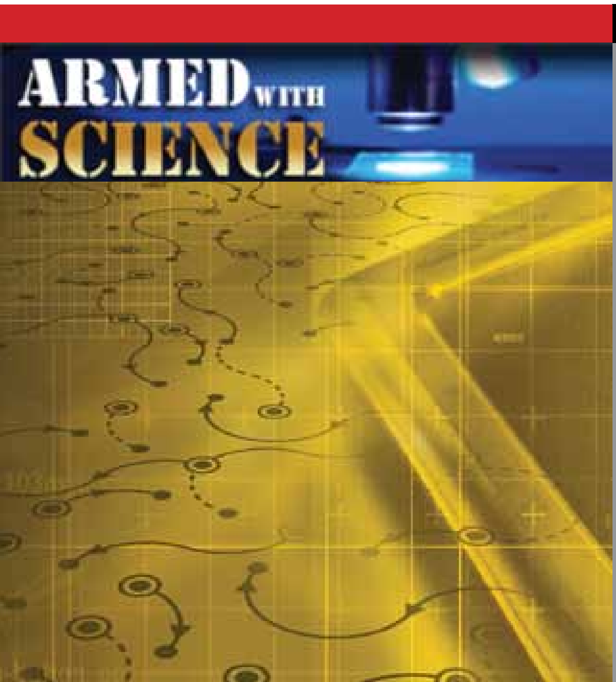
Mr. Frangiskatos is also the 2010/2011 course coordinator for the following courses—

- Computer Security and Risk Analysis
- Network Management and Security
- Web Engineering

Mr. Frangiskatos holds an MSc in Computer Systems/Software Engineering and several industry certifications including Cisco Certified Network Associate (CCNA) and Certified Information Systems Security Professional (CISSP). His research interests include network and computer systems security, forensics, and network and computer systems security exploitation. [1] ■

References

1. *http://www.cms.gre.ac.uk/staff/details.asp?id=416*



In January 2010, the Department of Defense launched a science and technology blog, *Armed With Science,* to continue its efforts to highlight the advancements military scientists and engineers are making in collaboration with the public. This blog provides another example of how DoD is improving its interface with interested citizens through social media, along with the wiki DoDTechipedia and the networking tool Aristotle. IATAC recently posted a blog entry called, "The Evolution of Information Protection" and looks forward to posting again in the future. If you are interested in seeing what's discussed on *Armed With Science,* visit *http://science.dodlive.mil/.*

2011 Information Assurance Symposium

by Kristin Evans

The Information Assurance Symposium (IAS) is the biggest, most informative conference IATAC attends each year. IAS 2011 was no exception.

IAS 2011 took place 7-10 March in Nashville, TN. Since this event was hosted by the National Security Agency (NSA), Defense Information Systems Agency (DISA), and the United States Cyber Command (USCYBERCOM), it brought together a wide variety of key players to discuss the most critical IA issues today.

At this year's symposium, the Department of Defense (DoD) Chief Information Officer (CIO) IA Awards were presented. These awards recognize military and civilian government personnel for their support of the DoD CIO Information Enterprise Strategic Plan (IESP). This year, there were eleven award recipients who were recognized for their efforts in furthering the objectives outlined in the IESP.

This conference allowed attendees to participate in one of five different IA tracks. These tracks delved into the significant challenges IA practitioners and leaders currently face and focused on how we may overcome these challenges collectively:

- Partnering for Strength
- Sharing Across Boundaries
- Prevent and Detect Attacks
- Cyber Readiness and Resiliency
- Information Assurance in Tactical and Contingency Environments.

Partnering for Strength

The highlight from this track was a presentation about encouraging increased collaboration across the U.S. government, industry, and centers of academic excellence. IATAC's mission is to share information across these sectors. However, doing so in practice poses significant challenges. This session addressed these challenges directly.

This track also included presentations about: how to meet future workforce needs across the cyber domain; legal challenges that continue to impact cyberspace; and a presentation about how IA Connect, an IATAC program, is helping to streamline the process of introducing new commercial products to government agencies.

Overall, this track highlighted how critical it is to leverage the best of what the private, public, academic and non-profit sectors have to offer, but it also highlighted the challenges of sharing information across sector boundaries.

Sharing Across Boundaries

This track included presentations about the technological solutions available to improve information sharing across boundaries, while also ensuring information remains secure and protected. It included presentations about identity and privilege management, and secure data enabling and tagging technologies.

The highlight of this track was the panel discussion that addressed "The Challenge of Synchronization." This panel addressed how technical and policy IA requirements and new mobile technologies impact each other, creating challenges for IA advancement. To realize true synchronization, requirements, policies, and solutions must complement each other. This panel took a look at how to allow them to do so.

Prevent and Detect Attacks

This track featured presentations by IATAC State of the Art Report (SOAR) author Karen Goertzel about how insider threat and the challenges affiliated with securing the information technology supply chain impact prevention and detection of cyber attacks. These presentations highlighted the research and analysis incorporated in IATAC's *Insider Threat* and *Security Risk Management for the Off-the-Shelf Information and Communications Technology Supply Chain* SOARs.*

This track included several sessions on various aspects of continuous monitoring as well as advances in analyzing malware. Most importantly,

▷▷ continued on page 31

Cyberspace Operations and the Need for an Operational Construct that Enables the Joint Force Commander

by Michael Collat

The exercise of command and control (C2) is the Joint Force Commander's (JFC) primary contribution to warfighting. C2 is what the commander "does." If the JFC does not understand the C2 systems, the JFC cannot effectively control them, and control of the C2 architecture is a basic requirement for exercising C2. [1]

How do we organize cyberspace operations in the DoD to leverage the efficiencies and authorities of national organizations that enable us to operate globally at "net-speed" while also allowing a regional JFC to exercise control over the C2 apparatus to balance technical and operational risk?

Over the last 15 years, the Department of Defense has recognized the criticality of decision superiority in enabling operational success and has understood the importance of reliable information networks to support decision-making and C2. The fragmented approach that the armed services and defense agencies take to fielding, operating, and maintaining operational networks (as well as the highly modular nature of information technology [IT] and Internet technologies) highlights the need for standardization to improve interoperability and efficiencies in delivering IT assets and network connectivity. In an effort to establish configuration control over this modular "plug and play" technology, the military services have consolidated responsibility for providing, operating, and defending networks at an enterprise level into functional, service-level organizations. While alignment of like functions has advanced the amount of control technology providers can exert in provisioning and operating the networks, it has also accentuated seams between the joint warfighters whose missions are ultimately dependent on network capabilities and their service providers.

> How do we organize cyberspace operations in the DoD to leverage the efficiencies and authorities of national organizations that enable us to operate globally at "net-speed" while also allowing a regional JFC to exercise control over the C2 apparatus to balance technical and operational risk?

Clearly, the efficiencies and configuration control of centralized provisioning must be preserved while simultaneously being responsive to warfighter needs that vary as the situation, phase of conflict, and tolerance for both operational and technical risk dictate. As net-centric warfare has evolved and cyberspace has become its own operational domain, the need for managing and satisfying the competing equities of centralized control and operational flexibility are as compelling as ever. This article shares the latest thinking from a geographic combatant command that has advanced the discussion within DoD concerning the roles, relationships, and responsibilities regarding command and control of cyberspace operations.

The U.S. Pacific Command (USPACOM) has long been at the leading edge of operationalizing network operations (NetOps), computer network defense, and cyberspace operations, guiding the evolution of the Theater C4 Control Center (TCCC) to the Theater NetOps Control Center (TNCC), the Theater NetOps Center-Pacific (TNC-P), and NetOps Analysis Cell (NAC) through the development of the Cyber Fusion Center (CFC) and the emerging CYBERPAC (Provisional) construct. As the initial effort, the TCCC pilot program defines the architectural framework required to execute NetOps

within the Pacific theater. Additionally, the TCCC provided a focal point for compiling information to help the USPACOM commander understand the status of all communications assets across the theater and their impact on theater operations.

This pilot effort was documented in a Concept of Operations that formalized the construct across the DoD as the TNCC, focusing on the functions of network management, information assurance, and information dissemination management. Recognizing the opportunity for synergy between theater and global NetOps entities, USPACOM and the Defense Information Systems Agency-Pacific (DISA-PAC) have combined efforts by merging their NetOps centers into the TNC-P. In order to complement the TNC-P with an analytical element to fuse functional expertise and assess operational impacts, USPACOM formed the NAC. The NAC advanced the command's analytic capabilities by integrating intelligence functions and critical infrastructure protection to bring threat and vulnerability components to operational risk assessments. The Cyber Fusion Center expanded this concept by focusing on full-spectrum cyber operations including synchronizing offensive cyber capabilities and integrating cyber decision support into USPACOM contingency planning processes. As an experimental concept for the exercise TERMINAL FURY 11, CYBERPAC (P) represents the next evolutionary step by further synchronizing theater and national cyber capabilities to enable the JFC.

Much of this development has been refined through integrating Information Assurance (IA) and cyber elements into exercises to examine emerging cyber concepts in an operational context. The success of this effort lies in not treating the cyber "war" as a separate fight, but instead integrating it into the other domains and presenting the JTF commander with the challenges that emerge from both the kinetic and non-kinetic operations. USPACOM's exercise TERMINAL FURY (TF) sets the example as the preeminent COCOM exercise integrating the cyber domain with the other warfighting domains; it has migrated cyber from a J6 staff focus to a command focus. For example, in recent exercises, USPACOM is credited with "breaking new ground" with the CFC construct for formalizing cross-functional collaboration between the cyber disciplines of intelligence, defense and offense. A subsequent exercise saw the addition of the Joint Cyber Operations Task Force (JCOTF) which deployed from the newly-established U.S. Cyber Command (USCYBERCOM), bringing needed cyber capabilities and national-level authorities in support of a simulated regional contingency. However, as the Commander's Summary Report notes, by not effectively integrating with established USPACOM contingency planning processes, the JCOTF presented the potential of actually disrupting the USPACOM decision-making process. The report recommends further clarifying the roles, relationships, and bed-down of USCYBERCOM forces sent forward to support USPACOM contingency operations to enable more effective integration into Joint Force Commander planning and decision processes.

USPACOM's exercise TERMINAL FURY sets the example as the preeminent COCOM exercise integrating the cyber domain with the other warfighting domains; it has migrated cyber from a J6 staff focus to a command focus.

The need for effective synchronization of USCYBERCOM and Geographic Combatant Command (GCC) cyber operations is rooted not only in the after action reports of the last two TERMINAL FURY exercises; it emanates from the recognition that cyberspace and joint force operations have converged and that operational success hinges on the JFC's ability to execute cyberspace operations effectively. Cyberspace provides not only the data and the information necessary to execute joint functions, but also the platform and capabilities to enable the conduct of joint operations. [2]

Currently, USPACOM and USCYBERCOM are jointly exploring establishing an organizational construct for TF11 to test the C2 relationships and processes needed to effectively matrix national and regional capabilities in support of a JFC.

Many options to manage cyberspace operations have been explored in recent years. One option is modeled on existing doctrine for operations in outer space, which by its nature is a global asset that cannot be partitioned or segmented for distributed control. This leads to a model with capability provided nationally and control retained almost exclusively at the national level, with very little flexibility to dynamically adapt the environment to support warfighter needs.

The previous USPACOM/J6, Major General Brett Williams, articulated the need to operationalize cyber in support of the JFC by stating that a global C2 model that is acceptable for peacetime enterprise efficiency is sub-optimal for wartime; global control does not provide the integration, responsiveness, and agility necessary to for cyberspace operations at the theater level. In his “10 Propositions Regarding Cyberspace Operations,” he acknowledges the global nature of the virtual domain, but argues for equal emphasis at the regional level. Put in other terms, the debates voiced in recent years over global versus regional control of cyberspace present a false choice; clearly, the challenge lies in designing organizational relationships that effectively manage the intersection of global enterprise operations AND regional joint force operations.

General Williams advocates for applying proven operational tenets and C2 models to cyberspace with the goal of providing the JFC direct operational C2 for theater-specific missions while allowing for global execution of other missions. He cites the Theater Special Operations Command (TSOC) construct as a model for a Theater Cyber Operations Command (TCOC) that would “provide the GCC with cyber capabilities in much the same way that TSOCs deliver special operations capability today. The TCOC would be under the combatant command (COCOM) of the GCC, and forces would be assigned or attached as appropriate. On a daily basis, the TCOC would be responsible for providing, operating, and defending the regional cyberspace architecture and would be capable of planning and integrating full spectrum cyberspace operations in support of contingency planning and crisis response.” Williams continues, “When required, the TCOC would accept additional forces and provide functional component command support to subordinate joint task forces. At the same time, the TCOC would respond to USCYBERCOM direction as the COCOM responsible for planning, synchronizing and executing global cyber operations. In addition, there would be an administrative command (ADCON) relationship with CYBERCOM for synchronization and standardization. … TCOCs could be established now with personnel already assigned to the theaters. The most challenging aspect of establishing TCOCs would be determining the C2 relationship between the TCOC and the service components.”

10 Propositions Regarding Cyberspace Operations
(with acknowledgement to Phil Meilinger's 10 Propositions Regarding Air Power)

1. Cyberspace is a warfighting domain. At the operational level of war, cyberspace operations are most similar to operations in the air, land, and maritime domains.
2. The Joint Force Commander (JFC) must have Command and Control (C2) of cyberspace just as he does the air, land, and maritime domains.
3. C2 of cyberspace is the key enabler for exercising operational C2.
4. Defense is the main effort in cyber at the operational level of war.
5. Cyber is the only manmade domain. We built it; we can change it. Creating a cyber Joint Operations Area (JOA) is the first requirement.
6. Cyberspace operations must be fully integrated with missions in the physical domains.
7. The JFC must see and understand cyberspace to defend it, and he cannot defend it all.
8. Networks are critical and will always be vulnerable. Disconnecting is not an option. We must fight through the attack.
9. Our understanding of non-kinetic effects in cyberspace is immature.
10. Understanding operational impact is the critical measure of cyberspace engagements.

Figure 1 This concept was originally presented by Maj Gen Brett Williams at TechNet Hawaii on 28 October 2010, since modified and current as of 22 December 2010

Currently, USPACOM and USCYBERCOM are jointly exploring establishing an organizational construct

The efforts of USPACOM, in partnership with USCYBERCOM and the U.S. Strategic Command, to define and test the relationships and operational processes among cyber organizations hold great promise to improve unity of effort and advance the DoD toward the vision outlined in this national military strategy.

for TERMINAL FURY 11 to test the command and control relationships and processes needed to effectively matrix national and regional capabilities in support of a JFC. This provisional organization is designated "CYBERPAC (P)," analogous to the Special Operations Command – Pacific (SOCPAC), which currently serves as a sub-unified command to USPACOM while maintaining an ADCON linkage to the U.S. Special Operations Command. As envisioned, CYBERPAC (P) will organize cyber forces currently assigned to USPACOM and will provide linkages into and relationships with national, theater, and allied NetOps, computer network defense, critical infrastructure protection, cyber intelligence, and offensive cyber operations capabilities. By effectively harmonizing cyber operations, intelligence, and planning functions, CYBERPAC (P) plans to synchronize regional and national cyber capabilities to provide effects that enable the Joint Force Commander. A recent Table Top Exercise (TTX) between USCYBERCOM, USPACOM, and many of the GCCs examined a draft C2 structure to accomplish this, with the goal of establishing relationships that can be exercised during TF 11. As currently envisioned, CYBERPAC (P) will focus on providing situational awareness, intelligence, planning, analysis, and decision support as well as command and control functions. Much of that capability will reside outside of CYBERPAC (P), either in theater organizations like DISA-PAC and the service components or at the national level through USCYBERCOM and the intelligence community but will be accessible *via* functional representation to CYBERPAC (P). Those linkages are currently being defined and will be further explored and refined using a TTX as well as through TF 11.

In 2006, an observation of the National Military Strategy for Cyberspace Operations read, "Cyberspace provides the foundations for C2 of military operations in other domains. C2 in cyberspace operations is achieving unified action vertically and horizontally, among all levels of war, throughout organizations." [3] The efforts of USPACOM, in partnership with USCYBERCOM and the U.S. Strategic Command, to define and test the relationships and operational processes among cyber organizations hold great promise to improve unity of effort and advance the DoD toward the vision outlined in this national military strategy. ■

About the Author

Michael Collat, CISSP | is an IATAC analyst currently conducting cyber defense analysis for the U.S. Pacific Command at Camp H. M. Smith, Hawaii. He has 23 years of information technology, cybersecurity, and intelligence experience both in private industry and as an officer in the U.S. Air Force. Michael holds a B.S. degree in Electrical Engineering from Lehigh University and an MBA from Boston University.

References

1. "10 Propositions Regarding Cyberspace Operations," Maj Gen Brett T. Williams, 2 January 2011
2. "Joint Concept for Cyberspace (draft v0.1)," 1 October 2010
3. "National Military Strategy for Cyberspace Operations," Chairman of the Joint Chiefs of Staff, September 2006

Attaining Security 2.0 and Beyond

by Chris Silva

IANS Research contributes our Ask the Expert column in each edition of the IAnewsletter. *In lieu of this column, Chris Silva presents this more in-depth look into how information security is evolving. We hope readers benefit from the insights this article presents.*

Empowering InfoSec with Research

These are among the many types of queries that IANS Research receives every day from end-user customers in the Fortune 100:

"How can I get my CEO to recognize the value of security in my organization?"

"What are the best ways to hire new security professionals for my security department?"

"What SIEM solutions should my organization choose to correlate events proactively, before they represent a serious issue?"

IANS Research is a market research company focused on serving the needs of user and vendor organizations in the enterprise information security space.

IAnewsletter readers may be familiar with the quarterly column "Ask the Expert," by IANS Research staff. The queries highlighted in this column are real requests for guidance and help on strategy from end-user customers. These queries and their resulting research make up a large part of the guidance that end-user customers rely on.

InfoSec Professionals – Who Are They?

IANS focuses on addressing the needs of information security professionals by focusing on the topics and issues that matter to three core constituencies of information security (Figure 1):

- **Security Management**—Increasingly, the Chief Information Security Officer (CISO) is seen as an office receiving more attention inside the business, a double-edged sword to be sure. CISOs inside mature firms are viewed as peers of others in the legal and financial realm (gone are the days where information security reports to the Chief Financial Officer [CFO] as a cost function) and, in some cases, a resource for the CEO.
- **Security Operations**—The folks "keeping the lights on" in security have seen their purview broaden

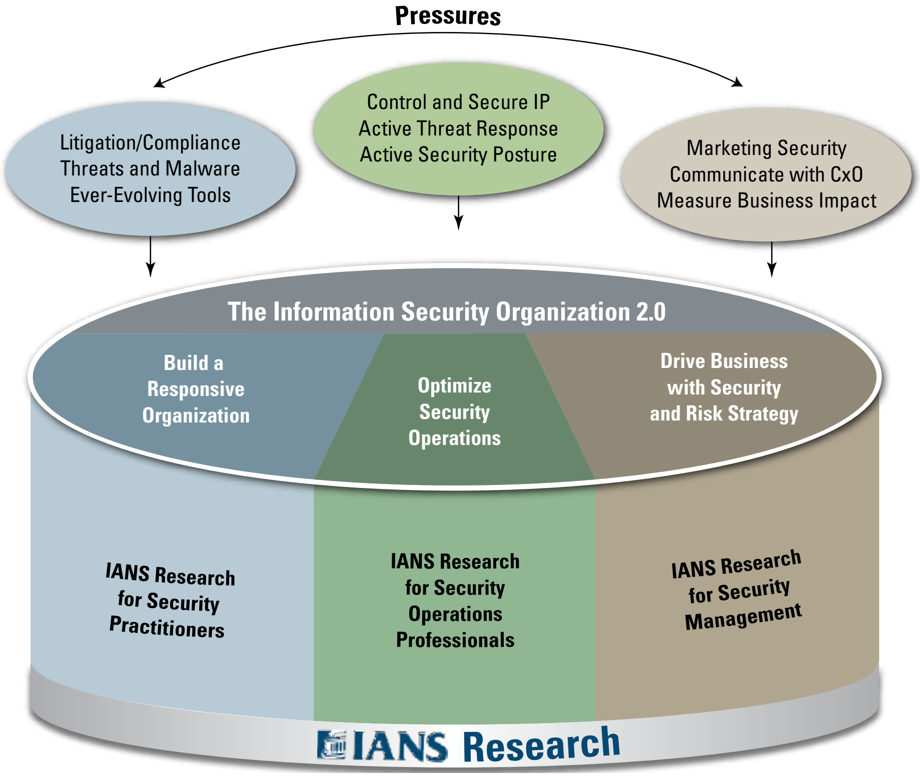

Pressures
Litigation/Compliance
Threats and Malware
Ever-Evolving Tools
Control and Secure IP
Active Threat Response
Active Security Posture
Marketing Security
Communicate with CxO
Measure Business Impact
The Information Security Organization 2.0
Build a Responsive Organization
Optimize Security Operations
Drive Business with Security and Risk Strategy
IANS Research for Security Practitioners
IANS Research for Security Operations Professionals
IANS Research for Security Management
IANS Research

Figure 1 Pressures on the information security organization

significantly in just the past couple of years as their decisions about how to keep the company safe while remaining productive mean they are increasingly looked to for a best practice solution for technologies the business requires. This represents a stark change from the past role of security as the "police" or "department of no," and means that baking security into policies and technologies designed to monitor the enforcement of those polices, while critical, must be transparent in many instances.

- **Security Practitioners**—This group is consistently growing year-over-year, but there are fewer and fewer broad examples of what the security practitioner "looks like;" this trend will likely continue. In organizations forced – because of a heavy compliance load, such as in financial services – to take a very proactive and business-centric approach to information security, entire departments of risk have been formed. In these and other verticals, we see the "security guy" as someone with a legal background or a deep understanding of criminal justice and threat profiling. This group grows to encompass the entire audience for all things external from legislation to nation-state-backed threat actors and wants to put a framework of risk around each.

The issues and needs of these groups vary. IANS has created a research calendar that addresses to the hot button issues of these groups (Figure 1).

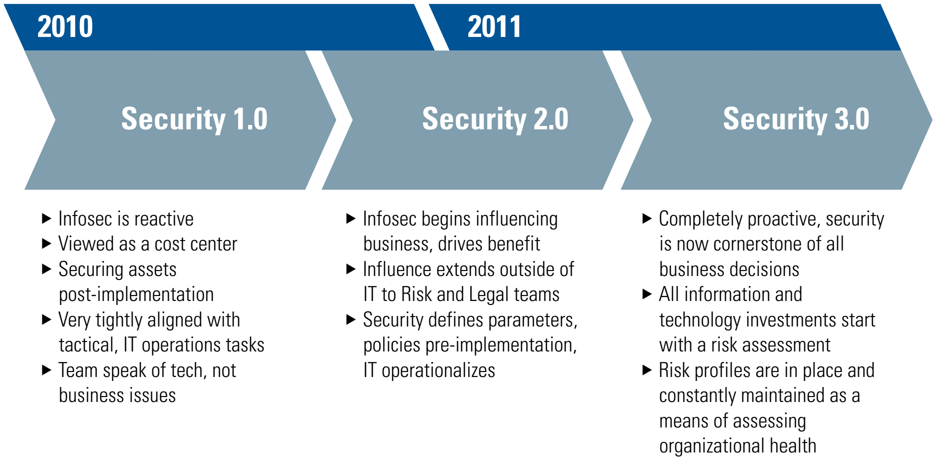
Attaining Security 2.0: A New Mandate

Over the course of 2011, helping companies to develop security organizations that are forward-looking, proactive, and tied closely with the business objectives of the larger business will be key. These new security organizations – Security 2.0 – as the name indicates, will not be a beginning state for most enterprises; rather they will be a mid-process transition from Security 1.0, where information security is a cost center, very much like information technology (IT) in more immature organizations, to Security 3.0 where information security is a fundamental building block of every business venture the organization takes (Figure 2).

Many organizations have moved beyond Security 1.0 and are already looking for ways to make their information security organization, its members, and its leadership an integral part of the business, driving the bottom line and making security a key part of the company's future.

Key Concerns? Management, Network, and IP Protection Top the List

Over the course of 2010, IANS conducted more than 500 Ask An Expert (AAE) queries submitted by its end-user clients. Across nearly 400 of these queries, while specific topics ebbed and flowed, managing security, securing the network, and information protection have remained the top themes. This may be due in large part to the new and



- Infosec is reactive
- Viewed as a cost center
- Securing assets post-implementation
- Very tightly aligned with tactical, IT operations tasks
- Team speak of tech, not business issues

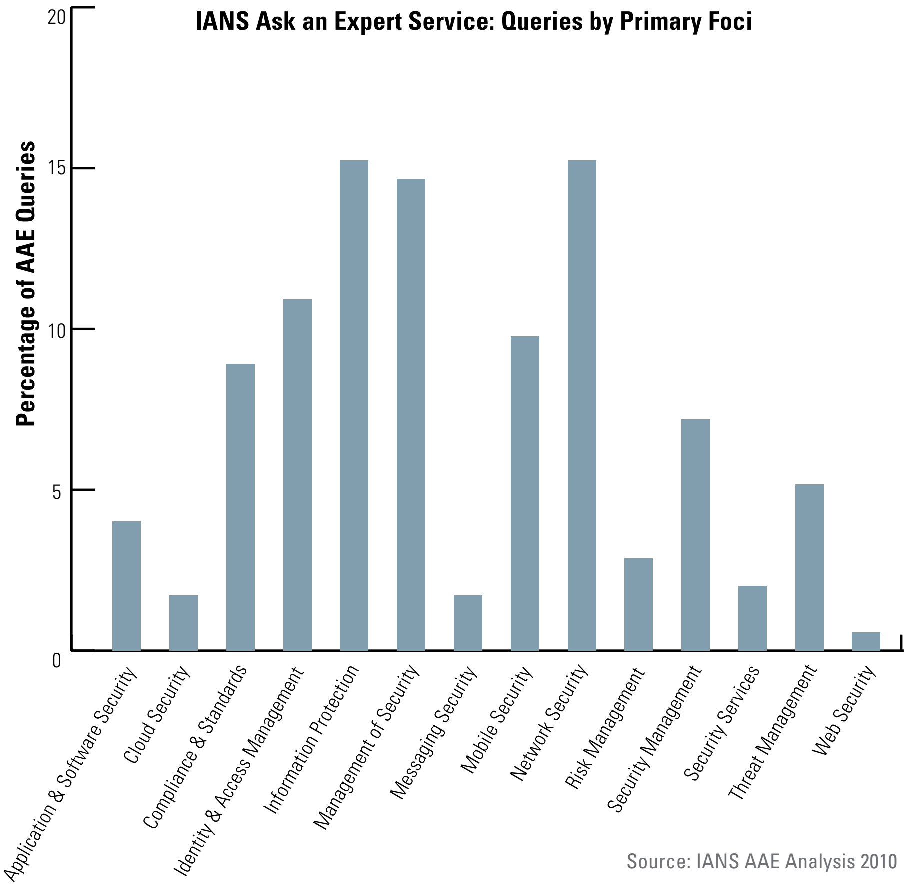
- Infosec begins influencing business, drives benefit
- Influence extends outside of IT to Risk and Legal teams
- Security defines parameters, policies pre-implementation, IT operationalizes

- Completely proactive, security is now cornerstone of all business decisions
- All information and technology investments start with a risk assessment
- Risk profiles are in place and constantly maintained as a means of assessing organizational health

Figure 2 Fundamental security building blocks, from 1.0 to 3.0

varying ways in which employees are pushing to use information inside and outside the firewall. What is the takeaway for 2010 based on these queries? Security must move from tactical to strategic, from task-centric to policy and business focused, and must do so with visibility and intelligence as the key tools. Insight into what data is being transferred, where it is being sent, and through what vehicle are the best weapons for an organization that aims to be primed to take on the challenges of diverse applications, from social media tools to mobile devices.

Some primary and secondary research foci include 27 subject areas that end users in information security want to know more about. A sampling of these subject areas include: compliance and standards, application security, threat management, firewalls, policies, and information protection (Figure 3).



Source: IANS AAE Analysis 2010

Figure 3 Queries by primary focus

In 2010, three of the primary focal points stood above all others in terms of representation among 2010 AAE queries:

- Management of security
- Network security
- Information protection

As we see organizations attempt to get smarter and more proactive about security, protect information, and build adaptive networks, it is important that security organizations take the following strategic steps:

- **Re-think the components of the security organization**—As organizations transition into Security 2.0, the makeup of the team from skill sets to background should shift away from the task-centric IT hires of the past to more risk and supply-side aware recruits. Position the security organization as an arbiter of policy and best practices with some technology guidance and leave the "operationalization" up to the IT operations team. Take a look, too, at metrics. Ensure that success is not measured in old IT terms but in business-centric "how-does-this help-the-larger-company" terms.
- **Think apps, not ports**—You've heard this before, and the constant *sturm und drang* from network equipment vendors trying to sell adaptable, next-generation solutions adds to the "strategic" cacophony. However, this noise is not simply marketing spin. A network that can distinguish an application that poses a threat based on context versus looking at port, source, and destination, serves an organization well, provided it is using tools like mobile, social media, and information sharing to drive the business instead of implementing *ad hoc,* unfamiliar solutions. The direction of network security should mirror that of the overall organization, create an environment that safely allows for the use of new tools as they drive greater efficiency in the business, and can do so without opening up security holes. Staying informed about traffic is key to staying secure.
- **Protect what counts**—2011 will be a year of more legislation and higher bars to crest on the compliance front. As businesses and individuals become aware of the amount of sensitive data that is being collected and stored, expect the burden of protecting data to increase. We're just now starting to see the backlash of location-enabling applications and maintaining detailed data stores on clients. It is time to take a look at that intrusion detection system tool that's sitting on the shelf and work it into a policy-backed information protection and retention solution, not just as a point product. A clear and consistent audit trail of what information is gathered, what is retained, and – also important

– what is not, will be at the heart of a prepared security organization in 2011 and beyond.

The Future: Security as a Foundation for Everything

While most information security organizations are undertaking a fundamental change to attain the future state of Security 3.0, there are still further hurdles to truly make security a fundamental part of the organizational structure of a business. Already, though, leading-edge organizations are taking some groundbreaking steps to build security into their brand. Some examples are the following:

- A CISO at a mid-size international financial services company is actively involving information security professionals in its sales process, marketing its capabilities and maturity in information security as a core element of its image as a trusted financial partner.
- A large IT services provider, believing in practicing what it preaches to disaster recovery and business continuity customers, has created a process for creating a risk profile for every IT investment or implementation that it undertakes, assigning a profile of systems impacted, likely outcomes, and requiring sign-off from a manager for each project to be approved.

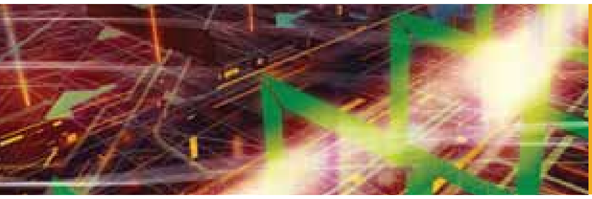
While it is a lofty goal for most organizations to achieve, and the examples above are from organizations that have taken many foundational steps from refining policies to honing a mix of technologies to support those policies, they serve as powerful examples of how information security, when foundational to the business, can drive change, improve the bottom line, and serve as a business differentiator.

This theme is one on which IANS plans to conduct multiple studies. Security 3.0 is a constantly evolving goal, changing to address the shifting winds of threat, legal and compliance climate, and business objectives.

It is critical for all IA practitioners to help usher in the era of Security 2.0, and beyond that 3.0, through actionable, targeted decision support. ■

About the Author

Chris Silva | is the senior vice president, research and service delivery, at IANS. In this role, Chris runs all daily operations of the IANS syndicated research and custom client advisory activities. Chris is committed to innovating the IANS research methodology to better serve security professionals. Chris comes from within the IT research industry and is a veteran of several established research businesses. He served four plus years at Forrester Research, most recently as a senior analyst working to serve security/risk and infrastructure/operations professionals. Chris is a graduate of the Isenberg School of Management at the University of Massachusetts.



Letter to the Editor

***One of our readers sent the following* Letter to the Editor *after reading "Workplace Privacy in the Cyber Age: Really?" in the Fall 2010 edition of the* IAnewsletter.**

I would like to bring to your attention two new Defense Advanced Research Project Agency (DARPA) research and development (R&D) efforts: Cyber Insider Threat (CINDER) and Anomaly Detection at Multiple Scales (ADAMS). Both look at insider threats, with the latter aiming at the range of employee activities and indicators, such as detecting the next Fort Hood shooter, and not just cyber events.

I find that too often the debate on privacy and surveillance assumes a binary outcome: mask employee information from scrutiny or permit administrators to view all activities. But these outcomes ignore the very real risk of abuse of authority and malicious activities by administrators, and even security and counterintelligence officers. Wherever possible, their access ought to be "need to know." One can be empowered, for example, to detect patterns of potential malfeasance without being given free rein to dig through message content. Automated tools for anomaly detection can help to promote privacy (by enforcing that need to know) while more scientifically ferreting out anomalous indicators, and tipping off human investigators. ■

The Move Beyond Green Pilot—the Sustainability Community of Interest

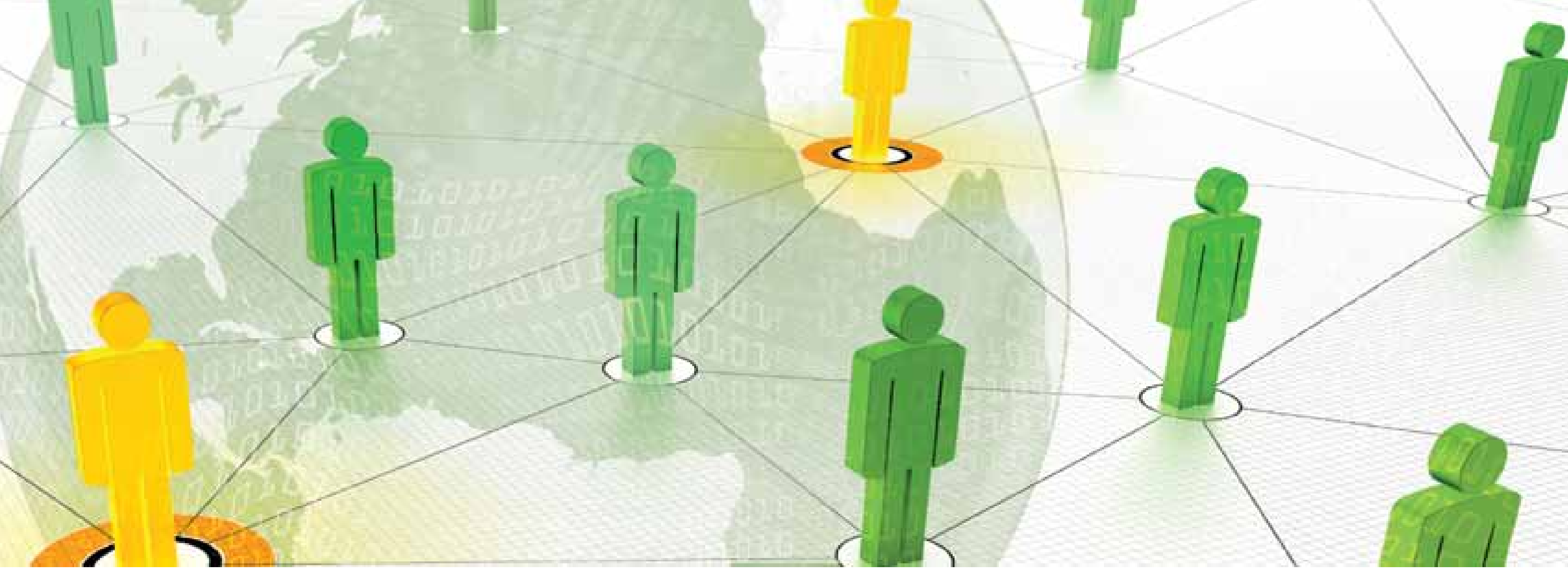
by Brian Smith

MBG is a Web 2.0-enabled site sponsored by the U.S. Army. It is modeled on a conversation and, like a good conversation, it is designed to be interactive and to have a breadth of opinions and perspectives.

In the spring of 2009, a team from the Army Environmental Policy Institute (AEPI) traveled to Garmisch, Germany, to meet with the staff of the George C. Marshall Center. The Marshall Center is a collaborative effort of the U.S. and German governments, whose goal is to build civil society in the former Warsaw Pact and Soviet Union countries through a robust in-residence program, distance learning courses, and continuing interactions with the alumni of the program. The goal of the AEPI visit was to discuss areas of cooperation between the Marshall Center and AEPI in the area of sustainability. As a result of this discussion, the AEPI decided to build a sustainability community of interest that would encourage the use of the topic of sustainability as an instrument of engagement. Beginning with a series of interviews with theoreticians and practitioners about their experiences in implementing sustainability, the Move Beyond Green Pilot (MBG) was created as a place to extend and expand the conversation, create connections, and build knowledge by creating an open and easily referenced set of source material and a forum for responsible and informed discussion.

MBG addresses a very basic issue for an organization looking to transform its fundamental way of operating. As the leadership of the organization defines the desired end state and the goals that the organization hopes to achieve, the rank and file of that organization must be able to address and solve day-to-day operational issues. In the case of sustainability, the challenge is to bring integrated and holistic approaches that address the economic, environmental, and social considerations into the decision cycle of managers and mid-level leaders across the organization. Transforming sustainability from concept to a way of doing business requires innovation, problem-solving skills, and solutions that may be missing from the organization. If those intellectual resources are not found organically, the search expands, identifying and connecting other pools of knowledge and experience as resources to be tapped. The solutions and approaches required to transform an organization to becoming sustainable must be identified, understood, and evaluated for their applicability at different levels and contexts across the organization. Doing so requires the ability to collect, organize, vet, and communicate potentially complex, context-sensitive information in an effective and efficient fashion. The consumers of the information must be able to access the information when they need it, appraise the integrity of the source, assess the accuracy and timeliness of the information, and they must be able to relate it to their understanding of the issue if they are going to be able to act on it.

MBG is a Web 2.0-enabled Web site that is part of an AEPI study on building knowledge about sustainability and using that process as an avenue for engagement. It is modeled on a conversation and, like a good conversation, it is designed to be interactive and to have a breadth of opinions and perspectives. One of the keys to making an organization sustainable is to build sustainability into decision-making processes across the organization. Sustainability



becomes the normal way of operating and facilitates the creation of a sustainability ethic that institutionalizes the desired behavior. In order for sustainability to become the norm, information must be consumable and accessible. All too frequently, the integrated and holistic nature of sustainable solutions and approaches involves a complexity of interaction that tends to lose the audience when presented in a conventional narrative. They know intuitively that being sustainable is the preferred approach, but being able to rationalize it and deal with numerous "what if" scenarios can make it a difficult path to follow. MBG was designed from the start to be a place on the Web where people can come to find good information, resources, and stories that relate the experiences of others with the express purpose of informing their own decisions about sustainability.

A story is a great method for communicating complex, context-sensitive information. As a general medium, it is consistent across time and cultures. By interviewing interesting people, creating new content at events, and commenting on the news of the day, MBG brings stories to an interested audience who are making decisions across a range of organizations that can benefit from becoming more sustainable. The conversation metaphor is important because conversation is how people share their stories and engage one another in the process of sharing and building knowledge. The site employs a number of different tools to collect, organize, and disseminate stories to its audience and, in many aspects, brings a social history of sustainability to the service.

Organizing and structuring information makes it easier to reference and to demonstrate the veracity of the source materials. Materials both cite sources and link to authoritative documents so readers can explore the context and the integrity of the source materials. By recording live events, MBG helps to create a record of speeches and pronouncements that can be revisited, referenced, and commented upon for greater clarity in the future. It becomes easier for an audience to make decisions from shared materials, and decisions are less dependent upon having access to specialized pieces of knowledge or insight. As more information becomes available, identifying and packaging it in useful ways becomes more important to its consumers. Web 2.0 technologies can be structured to help create context and build understanding of why something is important. Conversation and stories are successful vehicles because they bring context to data and bring structure to information. They help to create and communicate knowledge. Web 2.0 technologies allow the site to engage different media types and to bring a fuller picture of many of the activities being undertaken in the DoD community and the broader federal government while reducing the effort required to do so. Capturing presentations on important issues in video, for example, as opposed to traditional text transcriptions, helps to capture the emotive energy of the presenter and the more subtle

> Enabling the audience to interact with the material and with each other creates the opportunity for richer engagement; using COTS-based Web 2.0 tools reduces the barrier to entry for many and is becoming a more familiar way of interacting with information.

MBG employs a number of Web 2.0 tools, but the primary point of interaction with the public is the blog. The blog becomes the entry point for the site to help the audience identify what is new on the site and what may be interesting in the broader sustainability conversation.

communication cues that occur in a conversation. Identifying and quickly summarizing issues and articles addressing interesting topics, organizing libraries of material to make them easier to reference through tagging and tweeting events of relevance to a broader audience who may not have the opportunity to attend help to bring sustainability stories to those thinking about important issues and connecting them to people, organizations and efforts that may have been beyond their reach. Enabling the audience to interact with the material and with each other creates the opportunity for richer engagement; using COTS-based Web 2.0 tools reduces the barrier to entry for many and is becoming a more familiar way of interacting with information.

MBG is built on COTS software and services. It is a "subject"-focused site that uses current best practices to provide a positive and useful experience to its audience. It is staffed by a small team and uses a number of contributors with the goal of drawing on the expertise and experience of others and keeping the "voice" of the site varied and diverse. The editorial policy focuses on the quality of conversation and the richness of the story, and the staff strives to neither advocate nor endorse a particular product or position. The editorial team uses the Army's *Social Media Handbook* as a guideline in identifying, producing and posting its materials. It is designed to complement the customer's official site and focus more on knowledge creation and engagement around sustainability. MBG highlights the Army's and the overall Department of Defense sustainability-related activities by referencing official materials that might otherwise be obscured from the mainstream conversation about sustainability. MBG highlights its sponsors' activities as they apply to sustainability and tries to bring these activities into the mainstream conversation. The U.S. Army is a big organization, and understanding what it does in terms of sustainability requires an understanding of the institution, its missions, and how the broader public looks at issues of sustainability.

MBG employs a number of Web 2.0 tools to support its conversational storytelling, and the primary point of interaction with the public is the blog. The blog entries are composed by the contractor team supporting MBG and are then reviewed by contractor staff with Army Information Assurance training. All pieces receive a "two sets of eyes" review before being posted. The blog is used as the entry point to the site to help the audience identify what is new on the site and what may be interesting in the broader sustainability conversation. The site itself acknowledges AEPI as the pilot's funder and that the opinions expressed are those of the authors and not AEPI, the U.S. Army or the Department of Defense. This site is not an external official presence, so the materials are neither authoritative nor are they reviewed by the Public Affairs Officer. As a result, MBG cannot operate as a "dot gov" or "dot mil" site and can only reference official or authoritative materials. In addition to the blog, MBG hosts a collection of videos, a link library, a calendar of events, as well as its signature set of interviews. The MBG site has hosted webcasts of other AEPI events on sustainability. MBG also supports a Twitter feed, which further supports information collection and dissemination at sustainability-related conferences and public events such as the Environment, Energy, and Sustainability Symposium hosted by NDIA and the Pentagon's Energy Security event that features a range of speakers on sustainability efforts within DoD and the broader federal community.

AEPI looks at MBG as an experiment in using Web 2.0 technologies to support its mission of identifying future environmental issues of importance to the Army. As the pilot matures, it can be considered for a technology transfer to the government to meet a defined requirement and become a formalized channel for the government to collect and share knowledge on sustainability initiatives. By collecting information from a broad range of non-traditional and breaking sources, MBG enables them to access more and broader sources of information than would be possible otherwise. They gain experience in using more interactive technologies, expanding beyond their well-established Web site and offering capabilities to others within their organization. Gaining experience with Web 2.0 technologies helps AEPI to align with higher level mandates in executive orders on issues of transparency and engaging with the public. As the Army experiments with Web 2.0 and gains an understanding of how best to implement the tools within its own institutional culture, AEPI can create an understanding of how those same tools help it to execute its mission

▷ ▷ *continued on page 34*

Science Enhanced Networked Domains and Secure Social Spaces

by Dr. Carl W. Hunt

Globally accessible information networks enable rich interactions that create an environment for massive exchange of information, services, and goods. The underlying interactions of these exchanges create complexities that transcend our current ability to understand and secure the networked environments on which we rely. These complex socio-technical interactions also empower the interconnectivities that characterize what we call cyberspace. Media ecologist Marshall McLuhan noted in 1967 that "Environments are invisible. Their ground rules, pervasive structure, and overall patterns elude easy perception." [1]

In McLuhan's terms, we fail to perceive and therefore do not understand the emergence of human and machine-based behaviors that threaten the medium of cyberspace. We are missing a "science of cyberspace" that orients us to these threats and enables a more fundamental understanding of the environment. More than 40 years after McLuhan cautioned us, we find the same to be true of the most all-encompassing, interconnecting information environment known to man. In coming to grips with this new environment, we fail to appreciate the critical role that scientific concepts play, and we fall short in explaining and predicting the nature of the threats we face in terms that can help us resolve the "wickedness" of these challenges.

Cyberspace defense is not a U.S. problem, nor is it a government problem; in the end, it is a global, people problem.

In late 2009, the Air Force Institute of Technology's Center for Cyberspace Research began collaboration with what is now the Assistant Secretary of Defense for Research and Engineering's Rapid Reaction Technology Office to conduct research and an initial assessment of a project proposal to address cyberspace operations and security challenges. As a result of the initial assessment completed in December 2009, the study noted that the convergence of social and computer network-based operations produces an environment for the emergence of what are known as *wicked* problems. This project, originally titled Science-based Enhancements to Network Defense and Security (SENDS), addresses these wicked problems in the context of national prosperity and security in cyberspace.

In particular, cyberspace operational and security challenges are wicked problems because of the difficulty in framing effective questions and defining problems in a rapidly progressing, technology-driven environment. Responses to address the issues reflect little consistency because of the great number of stakeholder-users of cyberspace and the obscured ownership of the challenges. Rapid introduction of new technologies and user-defined processes aggravate these environmental challenges. McLuhan was absolutely right in 1967, even as he is now.

Cyberspace defense is not a U.S. problem, nor is it a government problem; in the end, it is a global, people problem. The social complexity ingrained in network operations and defense, spread across many users, causes fragmentation of thought. It separates underlying causes from potential solutions, a commonly identified symptom of wicked problems. In the case of cyberspace defense, technology serves as a substitute for scientific approaches and clouds the effects that science-based research brings to the challenges. In sum, technology competes with and even outpaces science.

Throughout human history, science has often lagged behind technology. The quest for efficiency over effectiveness sometimes led to tool and process development that provided "solutions" before we even knew the right questions. The same phenomenon appears to be true in cyberspace as we deploy technologies before understanding the true nature of cyberspace and those who interact within it both socially and professionally. To better orient ourselves, we require a "science of cyberspace" based on an ecological philosophy that helps us visualize interaction and interconnectivity.

A "science of cyberspace" leverages the convergence of the natural and social sciences towards a further shared understanding of how and what cyberspace truly is, both physically and socially. This science of cyberspace must be a transdisciplinary study in which we seek understanding of its physical, social, and organizational impacts on nearly all aspects of life on this planet. It must be a scientific discipline that explains and predicts the nature of the connected collectivity, exchange, and emergence that cyberspace enables, formalized through academic preparation and contribution. Such a study is just as necessary as the sciences that help us better understand life as a consequence and component of the physical environments of air, land, water, and space, and all their constituent parts. SENDS has this focus.

As we view cyberspace through science, we must also think of it in terms of an ecosystem. Similar to all ecosystems, cyberspace "self-seeks" equilibrium, a balance of the interactions, elements, and forces within it. We can look at the composition of this ecosystem as including human and network-based systems as the principle participants, incorporating the concepts of exchange and emergence, and "embrace" the outside forces of threats as ever-present. As any one of these elements changes, it affects the entire ecosystem, the components of which co-evolve in seeking equilibrium (Figure 1).

SENDS recognizes the complexity of both the definition and potential solutions relevant to the problem domain, the very nature of wicked problem management. It brings together business processes, education, technology, law and policy, modeling and simulation techniques, metrics, and most importantly, people to these challenges. Through this highly collaborative setting, SENDS accommodates the recognition and exploitation of emergence in cyberspace.

SENDS is nine months into a 12-month pilot study of cyberspace and cyberspace security in which we propose to explore what potential SENDS offers to DoD, the government, and to all users of cyberspace. We seek to develop what we call "open-source science" to address the challenges. Major contributing factors SENDS leverages include advanced modeling and simulation as a cyberspace laboratory, transdisciplinary perspectives, and educational curricula. As ecosystems adapt, so does SENDS, now known as Science Enhanced Networked Domains and Secure Social Spaces, to better account for the social nature of cyberspace, seeking to explain and predict as science should.

Across the entire scientific landscape of study, SENDS is integrating a transdisciplinary effort that seeks to explain and predict the nature of emergence and connectivity that cyberspace enables. The SENDS pilot program should demonstrate that a "science of cyberspace" is just as necessary as the sciences that help us better understand life as a consequence and component of the physical environments of air, land, water, and space. Publicly-accessible updates on SENDS are available at: *http://sendsonline.org.* ■

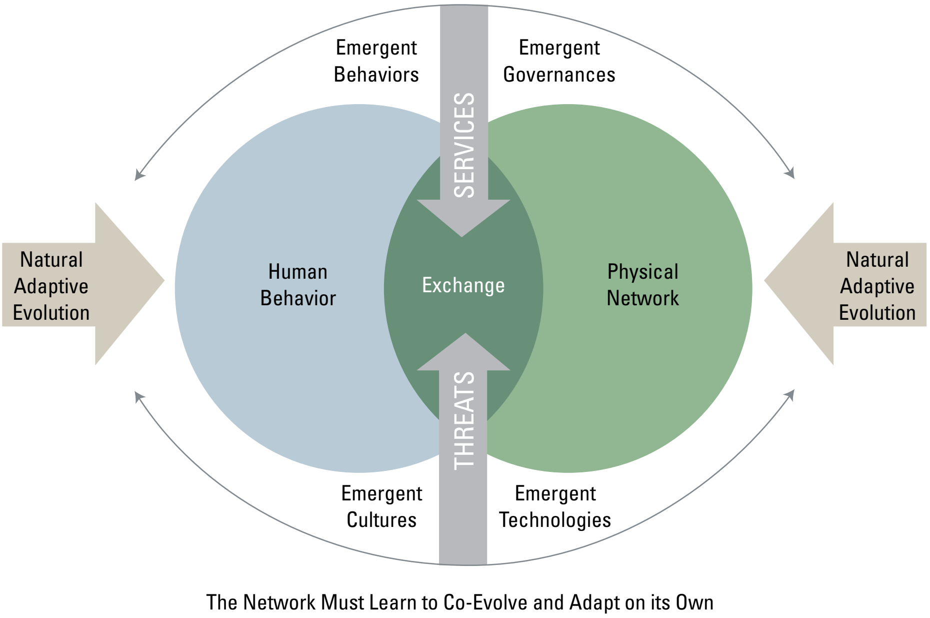


Figure 1 The cyberspace ecosystem

About the Author

Dr. Carl W. Hunt | is the senior research director for information operations for Directed Technologies, Inc. (DTI), of Arlington, VA. He is a founding partner in the Science Enhanced Networked Domains and Secure Social Spaces initiative (SENDS), co-sponsored by multiple U.S. government agencies. Dr. Hunt served 30 years in the U.S. Army, both as a military police officer and as an information systems technology officer and holds a Ph.D. in information technology from George Mason University.

References

1. McLuhan, Marshall. *The Medium is the Massage.* 1967.

▷ continued from page 15

ENHANCING THE GLOBAL CYBER DEFENSE WORKSHOP

and resources from workshop instructors, information pertaining to other training opportunities, links to information on international cyber events and conferences, a news feed, and a moderated discussion board.

By continuing to offer an enriching ICDW experience to registrants and encouraging participation from partner nations, industry, and academia, the Assistant Secretary of Defense for Networks and Information Integration (NII)/Department of Defense Chief Information Officer (ASD(NII)/DoD CIO) hopes that additional enduring partnerships with entities in the international cybersecurity domain develop and that current relationships can be strengthened.

The ICDW is conducted under the sponsorship of the International Information Assurance Program (IIAP), (Mike Coomes, director). The IIAP is a program component of the IA Policy and Strategy Directorate of the Office of the ASD(NII)/DoD CIO, Deputy Assistant Secretary of Defense (DASD), Identity and Information Assurance (IIA). The ICDW is executed in partnership with the Defense-wide Information Assurance Program (DIAP), IA Workforce Improvement Program, (George Bieber, director), and content providers from other U.S. defense agencies, academia, and industry. ■

For additional information, please contact Mike Coomes, director International IA program, ASD(NII)/DoD CIO, 703/571-5890, michael.coomes@osd.mil or Johanna Vazzana, ICDW program lead, 703/377-5085, iatac@dtic.mil.

About the Author

Johanna Vazzana | is an IA analyst supporting the ASD(NII)/DoD CIO International Information Assurance program. She manages the planning and execution of the International Cyber Defense Workshop.

▷ continued from page 17

2011 INFORMATION ASSURANCE SYMPOSIUM

the track highlighted a fundamental shift the IA community has taken from focusing on the strengthening of network defenses to detecting attacks before they can cause significant damage.

Cyber Readiness and Resiliency

This track focused on various aspects of trusted computing and incorporated presentations that addressed open source threats and how open source research can positively impact cyber readiness.

This track also featured a presentation on "Operational IA Assessments During Major Exercises." IA assessments during exercises provide a glimpse into the actual cyber readiness and resiliency of participating organizations. They are critical for determining cyber needs in real-world settings.

Information Assurance in Tactical and Contingency Environments

This track examined IA in real-world, wartime settings. It focused on how IA is having a critical impact on today's warfighter.

Sessions focused on communications in Afghanistan and the IA lessons learned from that theater of operations. They also focused on the criticality of interoperability and information sharing across the coalition of countries and organizations contributing to war efforts. IAS attendees had the unique opportunity to listen to speakers who have served in Afghanistan and have played important roles in implementing IA in support of combat operations. ■

IATAC looks forward to being a part of the solutions that address many of the IA challenges discussed at IAS 2011. For more information about IAS, please visit *www.iad.gov/events.*

*For more information about IATAC's SOARs and any other free IATAC reports, please visit: *http://iac.dtic.mil/iatac/reports.jsp.*

Data Clouds for Computer Network Defense

by Paul Brown, Aaron Cordova, and Jason Trost

Architectures for big data analysis

Network security systems will never have less data than they do today. Architectures are emerging that can facilitate storing, disseminating, and mining large amounts of data for the purposes of network security. These architectures and the capabilities they provide demand new ways of thinking about the tradecraft of data analysis, but they result in a fundamentally improved data analysis capability. This article covers some of the core principles surrounding cloud data processing and big data analysis and how they can be and are applied to improve network security systems.

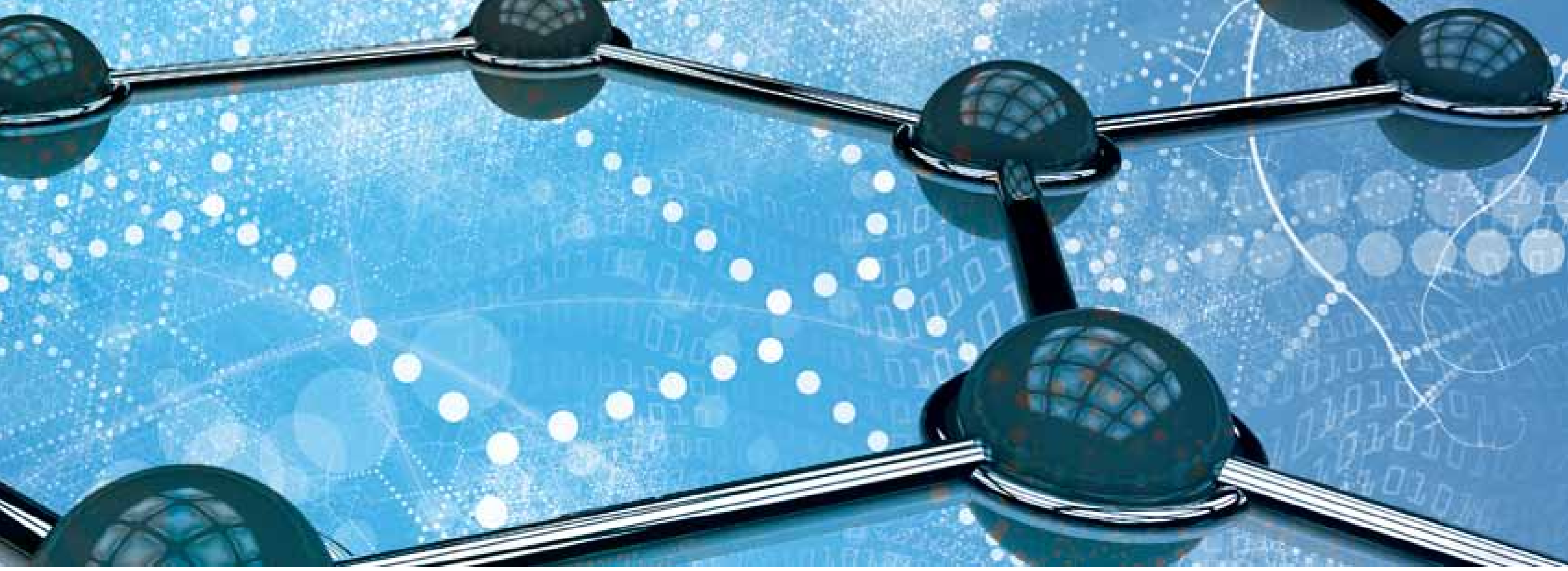
As the amount of data that corporations and governments have at their disposal increases exponentially, the traditional method of "scaling vertically," or adding more memory, central processing units (CPUs), and disks to a single system, has proven to be an expensive and insufficient option for meeting this ever-increasing demand. The result has been the emergence of architectures that "scale horizontally," gaining scale by leveraging large numbers of independent commodity computers. The critical feature of systems that follow this design pattern is that capacity scales linearly with cost. This feature, sometimes referred to as "horizontally scalable" or just "scalable," has a surprising impact on the design of architectures and analytics.

As the amount of data that corporations and governments have at their disposal increases exponentially, the traditional method of "scaling vertically," or adding more memory, central processing units (CPUs), and disks to a single system, has proven to be an expensive and insufficient option for meeting this ever-increasing demand.

There is a huge demand for "scalable" infrastructure components and as a result, various offerings have begun to emerge. They include distributed file systems such as the Hadoop Distributed Filesystem (HDFS), Sector, and CloudStore; distributed processing frameworks such as Hadoop, Disco, and Sphere; and distributed structured stores such as HBase, Hypertable, Cassandra, MongoDB, and Greenplum. Much of the complexity of operating in a distributed environment has been managed by these software components, freeing up developers to dedicate effort to the task at hand: in our case, analyzing network security data to find patterns, correlate information, detect emergent, anomalous behavior, and produce alerts. While there are a wide variety of infrastructure options to choose from, and discussing the pros and cons of each is beyond the scope of this article, each provides a unique set of advantages and drawbacks, allowing system designers to pick the components that best fit their unique requirements.

Network security

If best practices are followed for sensor deployments, including Network Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and other network and host-based sensors, large amounts of heterogeneous data can be produced. A thorough network security monitoring setup collects firewall logs, IDS alerts, host anti-virus logs, network flow records (Cisco Netflow or IPFIX), DNS query logs (Bind



logs), web logs (Apache or IIS logs), web proxy logs (Squid logs), web proxy cache (Squid's cache), web application firewall logs, DHCP logs, authentication logs, network utilization statistics, and possibly full packet captures (PCAP files). Also, as new network applications and services come online, new log files and formats must be included for comprehensive network security monitoring.

Traditionally, it has been a struggle to analyze and extract value from these diverse data sources in an efficient and coherent manner to enable computer network defense. Many corporations have encountered the problem of storing and processing vast amounts of heterogeneous data, and most have turned to cloud data processing technologies to solve this problem. The capability that cloud technologies offer – to co-locate these diverse datasets into one storage and processing system and aggregate and analyze them together – provides organizations with many opportunities for extracting relevant and actionable knowledge. The ability to store and process all data "at scale" is transforming how traditional businesses operate. Businesses use operational data mining to discover trends and patterns; it enables businesses to create value and services that were just not possible before. We believe these same benefits pertain if these tools and techniques are applied to computer network defense data.

More data leads to better answers and simpler analysis

With a "full take" of relevant computer network defense information and the ability to analyze it in the aggregate, it becomes possible to tackle previously intractable problems. Events that cannot be characterized by simple byte pattern matching can be illuminated using statistical analysis and data mining techniques. One example is detecting an adversary's attempts to "hide in the noise." With all data available for analysis, the chance is greater of detecting important instances of behavior that have easily been missed with limited or isolated views of the data. Similarly, low and slow network attacks such as low intensity scanning, distributed and coordinated scanning, targeted network reconnaissance, and some targeted exploitation attempts may produce a small number of observable events. These attacks may subvert a traditional IDS that has only limited detection capabilities and an isolated view of suspicious network traffic, but a big data architecture can ingest, analyze, and correlate all events and data, making detection much more likely.

Big data analysis is frequently made more effective by abandoning complex logical rules and letting the statistical properties of the data drive the algorithm. This results in simpler algorithms and better results. The simplicity of the distributed application programming interfaces (APIs) that are common today is a stark contrast to earlier approaches such as the Message Passing Interface (MPI) and other solutions that had a steep learning curve. This ease of adoption by developers allows subject matter experts to get their hands dirty and work with real data with a minimal up-front investment. Giving network defense experts a powerful and easy-to-use data analysis capability creates an ecosystem of innovation; the developers and subject matter experts get smarter as they explore the data, net capability development times shrink, and innovation grows.

Towards real-time analysis

In other domains such as business intelligence and web log analysis, data analysts often gather a large amount of data and process it as a series of batch jobs to produce useful result sets. The result sets are then loaded into traditional data stores to support *ad hoc* queries. In the security domain, batch analysis is useful for report generation, but there is also a need for real-time data analysis, detecting and stopping intrusions as they happen. Currently, this real-time analysis occurs within systems deployed throughout the network. Often, these systems employ

When all data within an organization can be combined and processed, and front-end detection methods are agile and holistic, businesses can detect threats faster.

complex rule-based triggers which require labor-intensive crafting by analysts with extensive domain knowledge.

As with Google's use of statistics to replace complex rules in automated language translation and anti-spam technology, the same opportunity exists within real-time network defense [1]. Utilizing the information gained from analysis of masses of historical data for real-time decision-making is a relatively straightforward process. It is accomplished by periodically producing summarized statistical models that capture the behaviors of interest, which are then used to statistically classify network events at the sensor. The models are compact, and the computation involved in scoring events is simple enough that it can be performed on network devices and allow for matching that is far more powerful than rule-based techniques. Models of known benign traffic can be used to detect anomalies, such as some forms of covert channel traffic, which may be undetectable by signature matching.

Conclusion

When all data within an organization can be combined and processed, and front-end detection methods are agile and holistic, businesses can detect threats faster. Events that may appear innocuous to an observer on the edge of the network are revealed as a coordinated threat when correlated and visualized across common dimensions such as time or network space. Events designed to be spread out over time and network space to evade detection can be reconstructed across a large enterprise. Statistical models based on a corpus of data can be created and utilized to detect nefarious behavior in real time.

Cloud data processing can enable next generation network security architectures. As organizations start to leverage data clouds for processing network and security event data, their network security postures will improve, and they will start collecting and processing more data. This same snowball effect has occurred in every field that has started using data clouds for processing and mining their data. ■

About the Authors

Paul Brown | is a lead associate at IATAC. His areas of expertise are big data analytics and cloud computing. He can be reached at *iatac@dtic.com*.

Aaron Cordova | is an associate at IATAC. He specializes in designing and implementing large scale data processing systems, big data analytics, and cloud computing. He received his B.S. in computer science, statistics, and linguistics from the University of Maryland. He may be reached at *iatac@dtic.com*.

Jason Trost | is a lead associate at IATAC. His area of expertise is designing and implementing secure distributed systems, network/security analysis, and cloud computing. He received his B.S. in computer science from Florida State University and his M.S. in information security from Georgia Institute of Technology. He is also a certified ethical hacker. He may be reached at *iatac@dtic.com*.

References

1. Google message security white paper. 2009. At *http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/a/help/intl/en/security/pdf/message_security.pdf.*

▷ *continued from page 28*

THE MOVE BEYOND GREEN PILOT—THE SUSTAINABILITY COMMUNITY OF INTEREST

and to support its parent organization with that understanding. ■

To learn more about MBG, visit us at *http://www.movebeyondgreen.com* or on Twitter at MoveBeyondGreen.

About the Author

Brian Smith | is the project manager for the Move Beyond Green Pilot. As a consultant and technical expert to the federal government, his areas of interest and practice include the application of Web 2.0 tools and open government solutions to improving decision quality, notably in the areas of environmental policy and sustainability. He holds degrees from Georgetown University and the University of California, Berkeley.

FREE Products Order Form

Instructions: All IATAC LIMITED DISTRIBUTION reports are distributed through DTIC. If you are not a registered DTIC user, you must do so prior to ordering any IATAC products (unless you are DoD or Government personnel). To register online: *http://www.dtic.mil/dtic/registration*. The *IAnewsletter* is UNLIMITED DISTRIBUTION and may be requested directly from IATAC.

Name ______________________ DTIC User Code ______________________

Organization ______________________ Ofc. Symbol ______________________

Address ______________________ Phone ______________________

______________________ E-mail ______________________

______________________ Fax ______________________

Please check one: □ USA □ USMC □ USN □ USAF □ DoD □ Industry □ Academia □ Government □ Other

Please list the Government program(s)/project(s) that the product(s) will be used to support: ______________________

____

LIMITED DISTRIBUTION

IA Tools Reports □ **Firewalls** □ **Intrusion Detection** □ **Vulnerability Analysis** □ **Malware**

Critical Review and Technology Assessment (CR/TA) Reports

□ Biometrics (soft copy only)
□ Configuration Management (soft copy only)
□ Defense in Depth (soft copy only)
□ Data Mining (soft copy only)
□ IA Metrics (soft copy only)
□ Network Centric Warfare (soft copy only)
□ Wireless Wide Area Network (WWAN) Security
□ Exploring Biotechnology (soft copy only)
□ Computer Forensics (soft copy only. DTIC user code MUST be supplied before this report is shipped)

State-of-the-Art Reports (SOARs)

□ Security Risk Management for the Off-the-Shelf Information and Communications Technology Supply Chain (DTIC user code must be supplied before this report is shipped)
□ Measuring Cyber Security and Information Assurance
□ The Insider Threat to Information Systems (DTIC user code must be supplied before this report will be shipped)
□ A Comprehensive Review of Common Needs and Capability Gaps
□ Software Security Assurance
□ IO/IA Visualization Technologies (soft copy only)
□ Modeling & Simulation for IA (soft copy only)
□ Malicious Code (soft copy only)
□ Data Embedding for IA (soft copy only)

UNLIMITED DISTRIBUTION

IAnewsletter hardcopies are available to order. Softcopy back issues are available for download at *http://iac.dtic.mil/iatac/IA_newsletter.html*

Volumes 12	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 13	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 14	□ No. 1	□ No. 2		

SOFTCOPY DISTRIBUTION

The following are available by e-mail distribution:

□ IADigest
□ IA/IO Scheduler
□ Research Update
□ Technical Inquiries Production Report (TIPR)
□ IA Policy Chart Update

Fax completed form to IATAC at 703/984-0773

IATAC

Information Assurance Technology Analysis Center
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171

Calendar

May

12th Annual New York Metro Information Security Forum (IANS)
2–3 May 2011
New York, NY
http://www.iansresearch.com/forums/splash.html?forum_id=57#p=main

Secure360
10–11 May 2011
St. Paul, MN
http://www.net-security.org/conference.php?id=416

June

23rd Annual FIRST Conference on Computer Security and Incident Response
12–17 June 2011
Vienna, Austria
http://conference.first.org/

NSA Mobile Technology Forum 2011
14 June 2011
Ft. Meade, MD
http://fbcinc.com/event.aspx?eventid=Q6UJ9A00P5GN

ISACA World Congress
27–29 June 2011
National Harbor, MD
http://www.isaca.org/Education/Upcoming-Events/Pages/World-Congress.aspx

July

Black Hat USA 2011
30 July–4 August 2011
Las Vegas, NV
http://www.blackhat.com/

August

7th Annual Government Forum of Incident Response and Security Teams (GFIRST) National Conference
7–12 August 2011
Nashville, TN
http://www.us-cert.gov/GFIRST/

DISA Customer and Industry Forum
15–18 August 2011
Baltimore, MD
http://www.disa.mil/conferences/

LandWarNet Conference 2011
23–25 August 2011
Tampa, FL
http://www.afcea.org/events/landwarnet/10/intro.asp

AFITC 2011
29–31 August 2011
Montgomery, AL
http://www.mc2-afitc.com/

To change, add, or delete your mailing or e-mail address (soft copy receipt), please contact us at the address above or call us at: 703/984-0775, fax us at: 703/984-0773, or send us a message at: iatac@dtic.mil