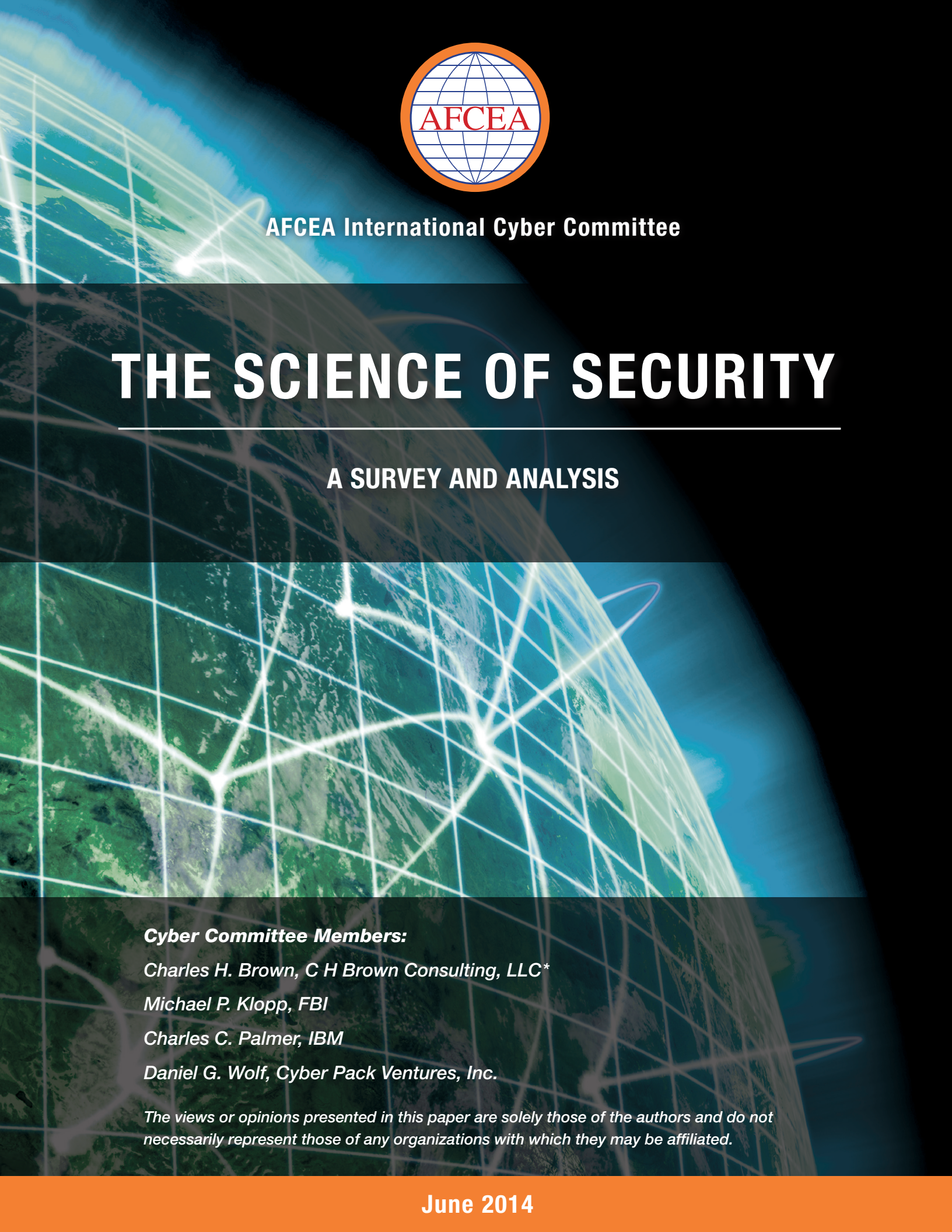


AFCEA International Cyber Committee

THE SCIENCE OF SECURITY

A SURVEY AND ANALYSIS

Cyber Committee Members:

*Charles H. Brown, C H Brown Consulting, LLC**

Michael P. Klopp, FBI

Charles C. Palmer, IBM

Daniel G. Wolf, Cyber Pack Ventures, Inc.

The views or opinions presented in this paper are solely those of the authors and do not necessarily represent those of any organizations with which they may be affiliated.

June 2014

WHY DOES THE SCIENCE OF CYBERSECURITY MATTER?

Virtually all societies throughout the world have become reliant on technologies we associate with the word "cyber." Whether it is traditional mainframe computation for financial and accounting purposes, networked devices for mobile communications, e-commerce or social media connections, real-time systems for command and control of military, utility or transportation systems or embedded medical devices, the quality of our lives depend on the correct operation of these systems. To be able to trust such complex systems requires we understand them. We have used science to help us understand, model and predict the natural world. It is tempting, therefore, to extend our thinking about science and nature into the more abstract cyber world. Thus the development of scientific principles and methods to increase our understanding of cyber-physical systems and to be able to measure and predict our trust in them has had both academic and commercial motivations for many years.

WHY DON'T WE ALREADY HAVE THIS "SCIENCE"?

Establishing a "Science of Cyber security" is a particularly vexing problem as neither term is well-defined.

At the Science of Security (SoS) Community Annual Conference (Hot SoS 2014) hosted at North Carolina State University (NCSU) on 8-9 April 2014, the following definition was offered by the government sponsored lablets[1] :

"The motivation behind the nascent Science of Security is to understand how computing systems are architected, built, used, and maintained with a view to understanding and addressing security challenges systematically across their life cycle.

In particular, two features distinguish the Science of Security from previous research programs on security.

- Scope. The Science of Security considers not just computational artifacts but incorporates the human, social, and organizational aspects of computing within its purview.
- Approach. The Science of Security takes a decidedly scientific approach, based on the understanding of empirical evaluation and theoretical foundations as developed in the natural and social sciences, but adapted as appropriate for the artificial science (in Herb Simon's term) that is computing."[2]

Science can either be seen as the logical extension of fundamental axioms to practical situations (deductive reasoning) or the generalization of experimental observed results (inductive reasoning). Most of us think of the natural world based on our observations. (The apple has always fallen from the tree to the ground. Thus it will always do so in the future.) But generalizing from a past set of observations is less useful in the cyber domain. (That store has always accepted my credit card in the past, therefore they always will in the future.) Our ability to use deductive reasoning as a tool of science is much less developed.

Cyber security itself is a similarly elusive term. One definition offered by Marcus Sachs is:
Cybersecurity (sic) is the process of risk reduction or mitigation as applied to the environment known as cyberspace. This process addresses attributes such as confidentiality, integrity, availability, authentication, and non-repudiation – and applies them to the data, information, and value created and exchanged in cyberspace by persons, organizations, and technologies existing in the physical environment.[3]

Physical security is generally well-understood because we generally understand both the physical objects involved and the physical threats to those physical objects. The cyber domain, however, is virtual and man-made, not natural. We are tempted to think of threats, either unintended or malicious, to cyber-physical systems as physical threats to the hardware. Threats to the data, processes or interfaces may cause loss of data, loss of availability or loss of trust, in addition to potential physical damage. Our inability to reliably and predictably measure and predict the consequences of these non-physical losses makes understanding cyber security even more difficult.

[1] http://www.nsa.gov/public_info/press_room/2014/lablets.shtml
[2] http://cps-vo.org/group/sos/hotsos2014
[3] Private communication, unpublished article, 2008.

WHAT PROGRESS HAS BEEN MADE?

An attempt at secure computation was one of the many pioneering accomplishments of the Multics project [1]. Many of the ad hoc protection mechanisms developed for Multics migrated into hardware, suffering inevitable performance penalties. The Bell and LaPadula model of data confidentiality and access control [2] was among the first to formalize the prior practice of the Multics experience. The US Government, through the National Computer Security Center developed a set of evaluation criteria known as the Orange Book [3] that subsequently became DoD and NIST standards. Almost two decades later Carl Landwehr noted the considerable attempts to produce formal models of provably secure systems had not realized their goal and our ability to model and predict behavior in computer systems remained a barrier to secure computation [4]. Ken Thompson's 1984 ACM Turing Award lecture "Reflections on Reflecting Trust" [5] highlighted the need to begin in a trusted state, meaning with trusted hardware and trusted software and to operate in a trusted manner, neither of which, he acknowledges, is practically possible. Recently, Peter Neumann of SRI has suggested we simply start over, taking better advantage of the additional architectural possibilities afforded by the availability of today's more capable hardware than was available when we first addressed the computer security problem [6]. There have been a variety of studies of a potential Science of Security. Perhaps most notable was the JASON study [7] that provided several observations:

> *"There is a science of cyber-security (sic). Because it is a science with adversaries, it uses, and will use, many different tools and methods. For the future, as far as can be discerned, there will be new attacks on old technologies, and new technologies that need to be defended." … The science seems underdeveloped in reporting experimental results, and consequently in the ability to use them. … Cyber-security is a problem that may be manageable, but not only is it not solvable, there's no agreement that it is being managed well."*

Schneider's article [8] provided a glimpse into the technical areas to which the laws of a science of security might relate, some examples of such laws, and how the science might be built up from existing knowledge and laws in computer science, mathematics, and physical sciences.

Prior to our initiating the AFCEA survey on the Science of Security (SoS), the government research community had already begun a study of academic institutions to identify and encourage activities promoting the SoS concept. Over the last couple of years, the government has made an on-going effort to advance research and academic study of SoS through the NSF-hosted Cyber-Physical Systems Virtual Organization (CPS-VO) Science of Security website [13]. There have been public and private initiatives to encourage fundamental research and education in the Science of Security (and related areas), but we had encountered none that sought the perspectives and plans, if any, of a group of technical organizations focused on government concerns around national security. This was the motivation for this survey of AFCEA members.

OUR SURVEY

WHO DID WE ASK?

The survey was sent to all AFCEA members. We felt that this community would be very interested in the science of security discussion. Further, we agreed that their employees and colleagues working in security technology, advanced technology, and policy would be among the most talented and visionary in the industry. One of these activities has been an ongoing government-sponsored survey of academic institutions to assess academic interest and activities related to the SoS concept. Part of this survey asked respondents to evaluate twenty statements to measure academic attitudes about SoS.

While the government's focus is on the academic community, it also has an interest in commercial attitudes and efforts related to SoS. In order to provide a comparable evaluation of attitudes, the government offered the statements from its survey for consideration of the AFCEA initiative in this area.

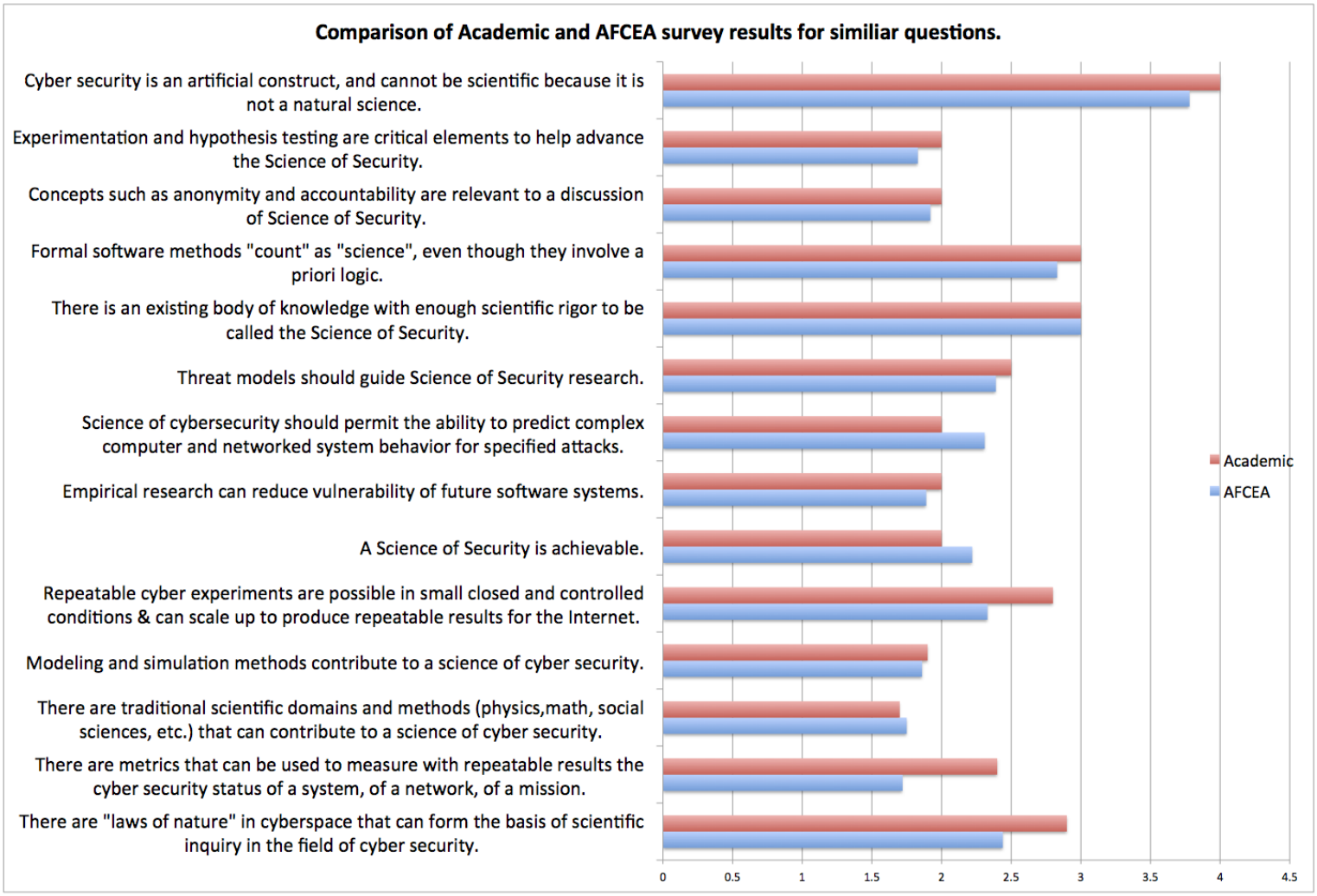
Of the twenty government statements, AFCEA selected fourteen for its survey and added another eleven that were considered relevant to the AFCEA community. These twenty-five statements were included in Question 1 of the AFCEA survey.

The following are the fourteen government statements with the corresponding AFCEA survey statement number indicated:

- There are "laws of nature" in cyberspace that can form the basis of scientific inquiry in the field of cyber security. (#1)
- There are metrics that can be used to measure with repeatable results the cyber security status of a system, of a network, of a mission.(#2)
- There are traditional scientific domains and methods such as complexity theory, physics, theory of dynamical systems, network topology, formal methods, mathematics, social sciences etc. that can contribute to a science of cyber security.(#3)
- Modeling and simulation methods contribute to a science of cyber security.(#4)
- Repeatable cyber experiments are possible in small closed and controlled conditions and can be scaled up to produce repeatable results on the entire Internet. (#5)
- A Science of Security is achievable. (#6)
- Empirical research can reduce vulnerability of future software systems. (#7)
- Science of cyber security should permit the ability to predict complex computer and networked system behavior in the face of specified types of attacks. (#8)
- Threat models should guide Science of Security research. (#10)
- There is an existing body of knowledge with enough scientific rigor to be called the Science of Security. (#11)
- Formal software methods "count" as "science" even though they involve a *priori* logic. (#12)
- Concepts such as anonymity and accountability are relevant to a discussion of Science of Security. (#13)
- Experimentation and hypothesis testing are critical elements to help advance the Science of Security. (#14)
- Cyber security is an artificial construct, and cannot be scientific because it is not a natural science. (#19)

The government survey is still on-going and is available at https://cps-vo.org/SoSSurvey

The following graph compares the results of the fourteen common questions from the previous academic and the AFCEA surveys.



1 = Stongly Agree
2
3 = Neither Agree nor Disagree
4
5 = Stronlgy Disagree

Note: The Academic survey is still accepting responses.
https://cps-vo.org/SoSSurvey

Reviewing the results of the academic and AFCEA surveys, only a few respondents indicated that Cyber security is not a science (#19).

There was lukewarm support for the following:

- There are “laws of nature” that apply to cyber security. (#1)
- Lab experiments can scale to the entire Internet. (#5)
- There is a body of knowledge that can be called the Science of Security. (#11)
- Formal methods “count” as science. (#12)

There was strong support for the following statements:

- Current disciplines contribute to cyber security. (#3)
- Science of Security is achievable. (#6)
- Anonymity and accountability are relevant. (#13)
- Experimentation and hypothesis testing are critical elements. (#14)

When results from these two surveys are compared, replication of results appears. A strong set of common answers points to the accuracy of the results.

Through this Science of Security survey, the AFCEA Cyber Committee was seeking to establish whether the respondents and their respective organizations had been thinking about, or actively addressing, the idea of a science of security. The intent of the Science of Security survey was to determine whether the cyber security field would benefit from having a commonly-held and mutually-agreed set of principles (a science) from which a practical set of metrics, standards and best engineering and implementation practices could be derived. Through such a science consistent and verifiable cyber security product and services attributes could be established which would benefit both producers and consumers as well as enable better procurement decisions.

We expected some respondents to have already begun work in the area and others to be considering it for future planning purposes. We expected the remainder with no current work in the area because (1) they considered it and decided against it, (2) they once had work in the area, but don't at present time, or (3) they have never considered it.

It should also be noted that each of the surveys had small sample sizes. This was likely due to the sensitive nature of some questions on the survey. Many recipients were unable to respond due to their organization's reluctance to share their private strategies and investment plans.

Broadly speaking, we asked five questions. Some had fixed responses from which to choose, and others allowed for free form responses.

WHAT DID THE RESPONDENTS SAY?

We arranged for the survey responses to be anonymous, to encourage free and open discussion. We also assume that some of those receiving the survey invitation passed it along to others either to answer for them or to add their own response. Thus, we have no way of correlating the thirty-six responses with specific organizations, missions, persons, positions, etc.

Question 1

For the first question, we provided a series of statements about a Science of Security. All thirty-six respondents answered this question, which asked for scaled responses ranging from "Strongly Agree", "Agree", "Neither Agree or Disagree", "Disagree", or "Strongly Disagree", along with a mostly unused "Don't know or Not Applicable" category for each statement.

Overall the results showed respondents felt that a Science of Security was feasible and that metrics for cyber security exist/are achievable. Over 80% of the respondents predicted that the Science of Security would enable new business models, such as cyber insurance. However, the same percentage agreed that the development of a science of security was indeed a long-term proposition.

Nearly all (89%) of the respondents felt that a variety of traditional scientific domains and methods could contribute to this science, including sociological and human factors research. The same percentage also agreed that anonymity and accountability, while somewhat conflicting concepts, are both relevant to the Science of Security discussion.

Question 2

For this question we asked whether the respondent's organization was actively pursuing, supporting, or considering research related to the Science of Security in some specific disciplines. Only 22 of the 36 respondents answered this question, which we assume may be the result of organizational confidentiality considerations. Of those 22 respondents, more than half responded that they were pursuing, supporting, or considering projects related to a Science of Security in Computer Science, Computer Engineering, Cyber security, Information Assurance, Software Engineering, and Systems Engineering. These results were not surprising, given the sorts of organizations that were invited to participate in the survey. However, these results were somewhat disappointing, in that without any further details on these projects, estimates of their potential impact on a Science of Security cannot be made.

Question 3

The next question was a follow-on to Question 2. We asked whether the respondent's organization had any other activities related to the Science of Security that were outside of the usual STEM disciplines, such as behavioral analysis, psychology, etc. This question received only 10 written answers from the 36 respondents. Of those, 3 respondents specifically offered "behavioral analysis projects," with sociology, psychology, and economics also mentioned. The remaining 7 respondents answered "No" to this question.

Question 4

For the fourth question we asked those who responded "yes" to Question 3 to provide a brief, non-confidential description of their associated research activity. This question received 8 responses, including the integration of business and threat intelligence, analysis of human behavior as an indicator of future malicious intent, real world system security improvement and flaw demonstration, "early warning indicators of malware" *(sic)*, and basic research. One response (self-identified as CACI) included the observation that "traditional Information Assurance and formal methodology has proven to be mostly academic and of little practical value."

Question 5

The final question of the survey asked the respondents for any further thoughts on a Science of Security. Nearly half of the respondents answered this question. Excerpts from some of the more interesting comments are included here:

- *The Science of Security focused on cyber elements must take into account Macro and Micro environments and social factors to address the fundamental problems of means and motivation.*
- *(a science of security) needs to be independent of the type of technology (OS, routers, s/w apps, etc.) used in order to be an (sic) true scientific study.*
- *Yes, a "science" and metrics can be developed that show repeatability, but this does not guarantee accuracy and a true reflection of cyberspace security.*
- *Even the basic of sciences will help inform the Balance of investment decisions (to include technology (hardware and software), solutions, tools tactics and procedures, training etc.*
- *Industry needs to take a strategic view of this challenge and not just develop tactical solutions for today's requirements.*
- *A science of security should take some of the guesswork out of identifying, monitoring and mitigating risks, thereby reducing costs, enhancing productivity, and ensuring greater national security.*
- *Data management is a key ingredient that must also be included.*
- *Including a social construction of science and technology framework in the research would add a valuable perspective*
- *We need to continue to invest in those areas that are knowable and use the science of security to de-emotionalize many factors by using research and empirical data*
- *Cyberspace is unique in that it's a man-made environment, but I'm firmly convinced that it obeys natural "laws" that are most likely discovered through advances in complexity theory rather than traditional physics or linear math. A parallel example is that without research into the math of structural engineering (tension, compression, torsion, etc.) combined with research into the materials of engineering (steel, wood, concrete, etc.) combined with investments in teaching engineering (Georgia Tech, MIT, CalTech, etc.) that all came together in the late 1800s we would not have any of the remarkable buildings, bridges, and other structures that enable our lives today. We would still be building beautiful cathedrals out of stone, but there would be no Golden Gate Bridge, no Chunnel, no 100+ story skyscrapers, and no 1000+ foot antennas. There would also be no aircraft, no spaceflight, and no massive concrete dams. So - in the cyber world we can keep building beautiful cathedrals and arch bridges out of stone if that's what we want to do. But we won't understand why they sometimes fall down and kill the occupants inside. We also won't understand the natural "laws" and forces that keep them standing, the nature of the materials they are built from, and certainly won't be able to move forward into new and exciting areas like skyscrapers and suspension bridges.*

CONCLUSIONS AND RECOMMENDATIONS

All man-made systems are vulnerable to unintended performance because of the mistakes/oversights of the system specifier, designer, implementer, tester, maintainer, or the end user. Those flaws are exposed by humans either by accident or on purpose, and often as result of the actions of others or natural phenomena.

The respondents to this survey and the government sponsored survey agreed on several key points.

- This is one of the few sciences with an endless supply of adversaries striving to find ways around the basic principles or "laws or nature" defined by the science.
- A science of security will not be solely concerned with technology. It is truly a multi-disciplinary effort, including in no small part the actions of humans. The actions of humans throughout the lifecycle of computer systems and networks, whether hostile, inadvertent, or due to ignorance, are the direct cause of the vast majority of security exposures and incidents.
- As with any science in its infancy, particularly one crossing multiple disciplines, initial progress will require a long-term effort. Thus, most industrial labs, such as those represented by most AFCEA members, will be unable to support a long-term commitment required for the birth and early development of a new science through their usual project processes. Given this, along with the broad economic, societal, and national security impact that progress in this area would have, it should likely fall to the US Government to support this work in academia, and in major industrial and government labs.
- Policymakers and users need help understanding just what a Science of Security would (and would not) mean.
- A science of security could result in real, measurable economic impact to the US economy and national security.

Several of the respondents indicated that their organizations were already investing in research in areas directly related to a science of security and that they were planning to continue to do so. This mode of strategic thinking is common among AFCEA members and the academics targeted by the government-sponsored survey. This is reassuring, as these are some of the most capable organizations likely to pursue Government support for work on this topic.

APPENDIX A: THE SURVEY

THE SURVEY USED FOR THIS EFFORT IS REPRODUCED HERE.

1. Below are a series of statements about the Science of Security. Please indicate your agreement or disagreement with the questions using the scale:

5=strongly agree
4=agree
3=neither agree nor disagree
2=disagree
1=strongly disagree
0=don't know/not applicable

- There are "laws of nature" in cyberspace that can form the basis of scientific inquiry in the field of cyber security.
- There are metrics that can be used to measure with repeatable results the cyber security status of a system or network.
- There are traditional scientific domains and methods such as complexity theory, physics, theory of dynamical systems, network topology, formal methods, mathematics, social sciences etc. that can contribute to a science of cyber security.
- Repeatable cyber experiments are necessary for a science of cyber security, are possible in small closed and controlled conditions and can be scaled up to produce repeatable results on the entire Internet.
- A basic science of cyber security is achievable.
- Empirical research can reduce vulnerability of future software systems.
- A science of cyber security would enable the prediction of complex computer and networked system behavior in the face of specified types of attacks.
- As long as people are part of our computing infrastructure, a science of cyber security will remain elusive
- Threat models should guide science of cyber security research.
- There is an existing body of knowledge with enough scientific rigor to provide a basis for a science of cyber security.
- Formal software methods can provide a realistic basis for a science of security.
- Concepts such as anonymity and accountability are relevant to a discussion of science of security.
- Experimentation and hypothesis testing are critical elements to help advance the science of security.
- A science of security would make procurement decisions easier.
- A science of security will have to include sociological and human factors/usability concerns.
- Development of a science of security will be a long-term proposition.
- A science of security would enable new business models, such as cyber security insurance?
- Cyber security is an artificial construct, and cannot have a scientific basis because it is neither a natural nor a physical science.
- A science of security should be investigated by academic institutions.
- A science of security should be investigated by the private sector.
- A science of security should be investigated by the public sector.
- A science of security would not result in increased regulatory oversight.
- A science of security would lead to improvements in protecting individual privacy.
- A science of security necessarily includes changes to existing laws and regulations.

2. Is your organization actively pursuing, supporting, or considering research related to the science of security in any of the following disciplines (Select all that apply):

- Cognitive science
- Computer science
- Computer engineering
- Cyber physical systems
- Cyber security
- Electrical engineering
- Electronics
- High performance computing
- Information assurance
- Mathematics and statistics
- Programming
- Scientific computing
- Software engineering
- Systems engineering

3. Do you have any other activities relating to the science of security that are not within the typical STEM disciplines, such as behavioral analysis, psychology, etc. ?

- (free form input)

4. If you answered yes to any of the above, please provide a brief description of the associated research activity if possible. We realize this maybe privileged information and we will treat it accordingly, however to not provide any company confidential information.

- (free form input)

5. Do you have any other thoughts on a science of security?

- (free form input)

REFERENCES

[1] www.multicians.org/security.html

[2] Bell, David and LaPadula, Leonard, “Secure Computer Systems: Mathematical Foundations” (1973)

[3] csrc.nist.gov/publications/history/dod85.pdf

[4] Landwehr, Carl, “Formal Models for Computer Security’, ACM Computing Surveys, Vol. 13 No. 3, September 1981

[5] Thompson, Ken, “Reflections on Reflecting Trust” Communications of the ACM, Vol. 27 No. 8, August 1984

[6] Neumann, Peter and Watson, Robert, “Capabilities Revisited: A Holistic Approach to Bottom-to-Top Assurance of Trustworthy Systems, Layered Assurance Workshop, Austin, TX, 6-7 December 2010

[7] “*Science of Cybersecurity*”, JASON, November 2010, The MITRE Corporation. 09 April 2014 at http://www.fas.org/irp/agency/dod/jason/cyber.pdf .

[8] Schneider, Fred B. “*Blueprint for a science of security*”, The Next Wave, Vol. 19 No. 2, 2012, pp. 47- 57; 09 April 2014 at http://www.nsa.gov/research/_files/publications/next_wave/TNW_19_2_BlueprintScienceCyber security_Schneider.pdf .

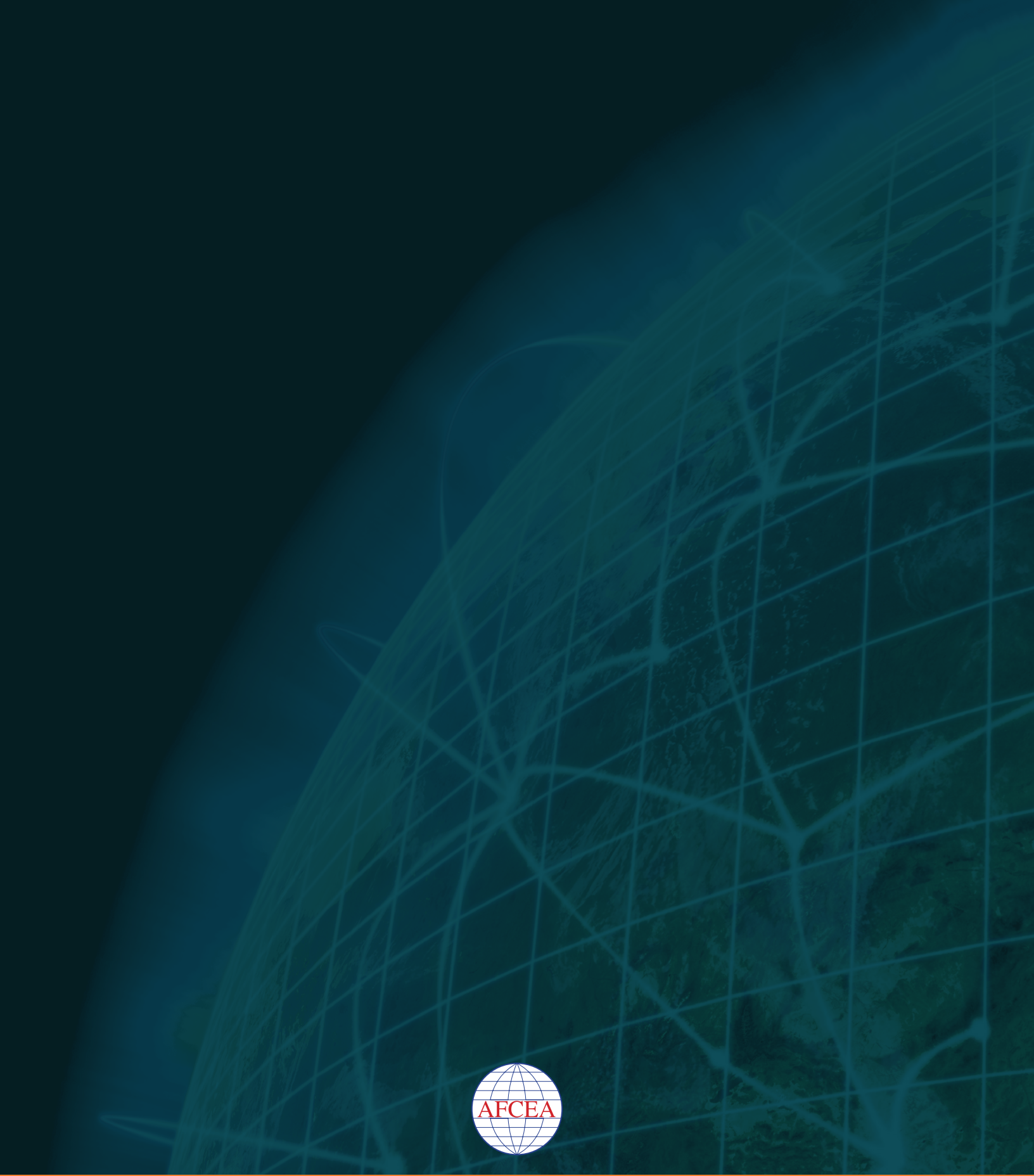
[9] Schell, Roger R. ;“Computer Security: The Achilles’ Heel of the Electronic Air Force?”, Air Force University Review 30(2), at http://www.airpower.maxwell.af.mil/airchronicles/aureview/1979/jan-feb/schell.html

[10] World Economic Forum, “Risk and Responsibility in a Hyperconnected World”, January 2014, at http://www.weforum.org/news/increased-cyber-security-can-save-global-economy-trillions .

[11] Lewis, James A., Baker, Stewart: “The economic impact of cybercrime and cyber espionage”, July 22, 2013, at http://csis.org/publication/economic-impact-cybercrime-and-cyber-espionage .

[12] Rowe, B., et.al.; “Economic Analysis of an Inadequate Cyber Security Technical Infrastructure”, National Institute of Standards and Technology Planning Report 13-1, February 2013, at http://www.bldrdoc.gov/director/planning/upload/report13-1.pdf .

[13] Cyber-Physical Systems Virtual Organization (CPS-VO) Science of Security website at https://cps-vo.org/group/SoS



The AFCEA International Cyber Committee White Paper Series

www.afcea.org/committees/cyber