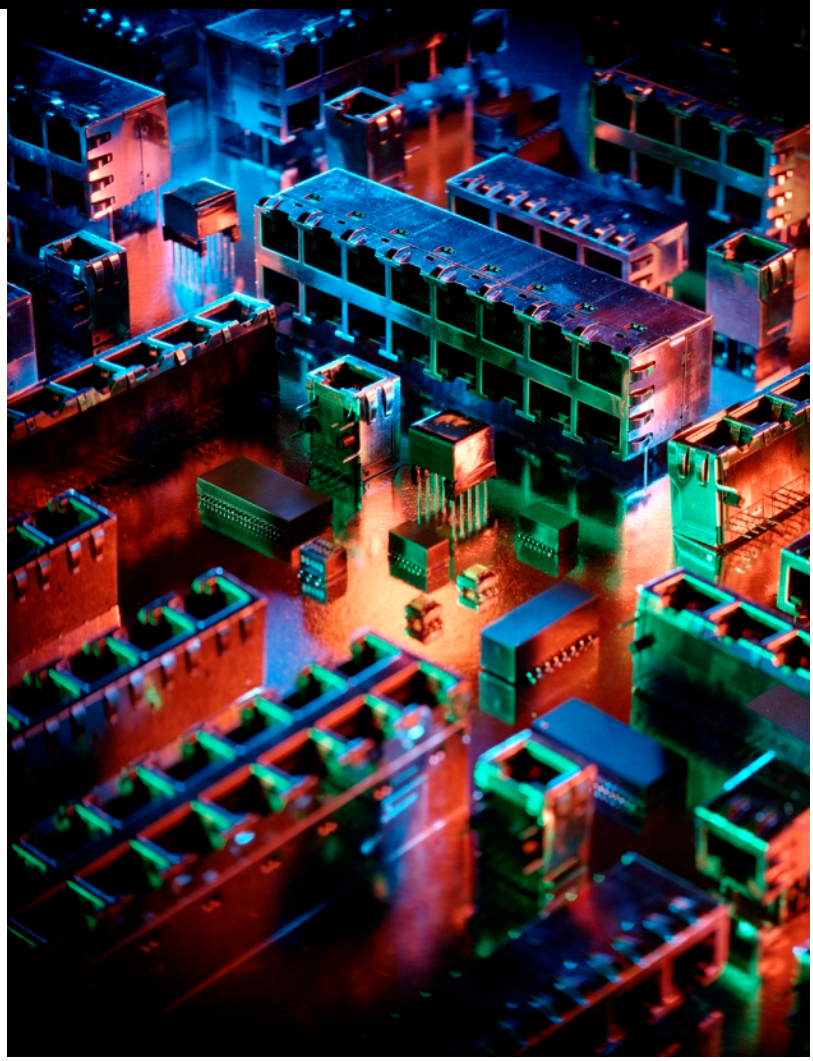
Multilateral Cyber Security Solutions: Contemporary Realities



— BY A.M.RUTKOWSKI,[1] W.A.FOSTER,[2] S.E.GOODMAN[3]

Cyber security poses one of the more significant contemporary challenges today, resulting in the deployment of enormous resources and its treatment in countless papers and reports. Inevitably, the subject of multilateral solutions is treated—suggesting the need and efficacy of pursuing or evolving various forms of global agreements and activities. One of the more comprehensive recent analysis is the now two-year old Sofaer-Clark-Diffie paper from the U.S. National Research Council Committee on Deterring Cyberattacks, Workshop on Informing Strategies and Developing Options.[4]

Using that paper and other related material as a starting point, we examine the nature and evolution of international collaborative activity related to cyber security since its publication — with a focus on multilateral solutions. Our brief report here is intended as an examination of the different forms of multilateral cooperation via the various institutions in the context of the extremely complex domain of cyber security. The different forms may provide better or worse contexts for achieving, or not achieving, various forms of risk reduction and agreements on what constitutes bad behavior in cyberspace.

There are two points emerging from this examination. The first is that in the realm of cyber security, a formal multilateral group with a huge mixed membership like the International Telecommunication Union (ITU) is not the place for operational security activities. Communities of trust in cyber security are both endemic and essential —many highly compartmentalized. This essential need is not found in more generic multilateral venues. The second point is that emerging functional cyber security platforms are "triple use." The same platforms that are essential for network management and for cyber security, are also used for surveillance by all governments. These three uses inherently engender very different trust communities that are context dependent and evolve through time—sometimes abruptly. It should also be pointed out that these platforms can be used by all manner of nimble criminal or antisocial actors.

This article also describes what appear to be new important attributes and constraints on that activity which inevitably limit and shape future multilateral solutions. This includes cyber security platforms that have emerged such as Continuous Security Monitoring as well as the increasing use of extraterritorial action to deal with non-state actors.

Cyber Security Fundamentals

At the outset of any review of cyber security—given the myriad different abstractions in use—it is essential to describe a definitive construct for purposes of its treatment here.

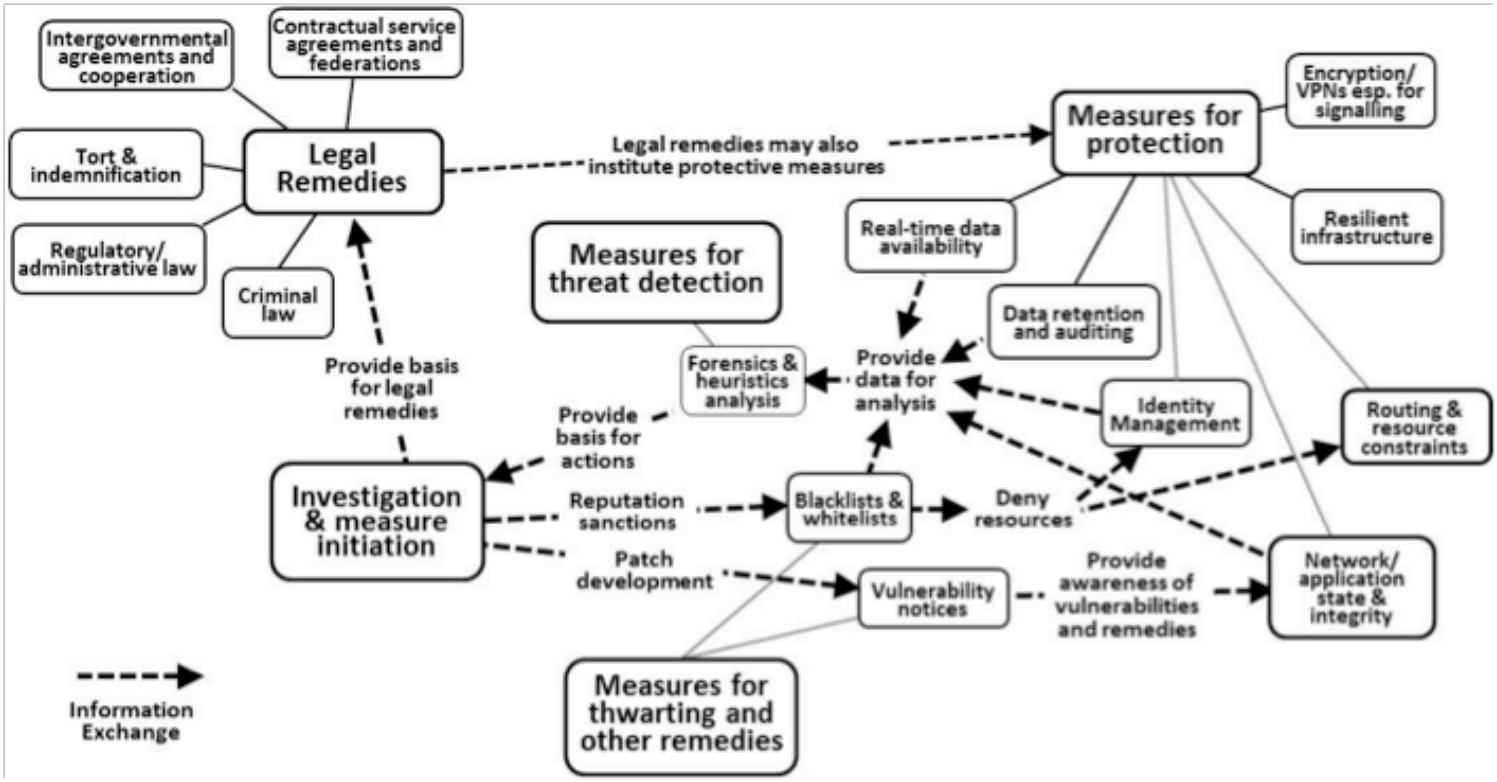


Figure 1. A model for describing cyber security.

The definition provided here is a simplified derivative of the many complex ones that have been formally adopted.[5]

Cyber Security consists of sets of techniques, policies, and activities intended to enhance trust and mitigate vulnerabilities inherent in the complex networked devices and services that permeate our lives today.

The Lukasik-Goodman-Rutkowski graphic depiction, developed four years ago, is also helpful in portraying what techniques and activities are comprised by cyber security. The diagram depicts cyber security as five clusters of interrelated activities: measures for protection, measures for threat detection, measures for thwarting and other remedies, investigation and measure initiation, and legal remedies. Highly dynamic and time critical information exchanges occur among the components of this highly distributed, autonomous cyber security ecosystem.

The model is essential because of an emergent reality. All of the devices that constitute or are attached to our information communication networks today consist of ever increasing numbers of subcomponents and executable lines of code to provide some exponentially growing numbers of services, applications and other functional capabilities counted in the millions. There are billions of such devices. All of these entities are continuously and autonomously changing—facilitated by openness in most networked devices and services that further exacerbate the complexities and vulnerabilities. The sheer number of potential threats and exploits in this environment preclude them ever being known. They also remain constantly evolving, ubiquitous, and persistent.

Added to this mix of system vulnerabilities and threats are institutional and human elements. Actors ranging from nation states to isolated individuals are capable of creating or exploiting vulnerabilities in these environments. Indeed, a knowledgeable insider in even an otherwise closed network environment is frequently one of the most difficult threats to detect and remedy. The result is a constantly changing exercise in risk assessment and reduction.

Absolute or even a strong measureable form of security is not possible. Important members of the cyber security community announced in December 2011 that that "there's no such thing as 'secure' any more..."[6] Subsequently much of the cyber security community has settled on Continuous Monitoring (CM) as the best we can do on a large scale at this time.[7] CM itself consists of numerous platforms such as Security Content Automation Protocol (SCAP) and an array of related assurance and incident exchange standards and practices designed to accomplish three things:

(1) constantly assessing the risk state of all devices and systems,

(2) constantly watching for threats,

(3) effecting remediations as soon as possible.

It assumes that there is no absolute security, and that the best we can do is manage risk. The Continuous Monitoring platform is the principal ensemble mechanism for advancing all of these capabilities. Underpinning the CM ensemble are structured information

Collateral Effects of the Continuous Monitoring Paradigm

Continuous Monitoring has arguably emerged as the principal viable approach for dealing with cyber security on a global scale. This new paradigm also has the collateral effect of reshaping and constraining multilateral solutions. The benchmark test for all multilateral solutions is: do they reduce cyber security threat risks. Unfortunately many multilateral organizations are ill equipped to do this operationally. While such organizations may have the capability for getting agreement on broad goals in legislative settings or even common specifications, they are not only ineffective at operational roles among compartmentalized trust communities, but also may adversely affect the risk equation by possibly adding more threats from the interposed multilateral organization itself.

For example, intergovernmental organizations in particular are highly vulnerable to insider treats. Organizations are beholden to fixed requirements for established nation states that treat all countries and their staff as equal and at the same trust level. Because staff are sponsored and approved by their nation states, the result is that broad global multilateral organizations in the UN system have rather low trust levels that presume the existence of extensive insider threats. North Korean staff is assumed to have the same trust level as staff from the United Kingdom.

The concerns here are not new. The Sofaer-Clark-Diffie analysis treated a number of requirements to improve multilateral organizations. One factor was "trust." They noted that cyber security is highly dependent on dynamic trust communities. The analysis noted that the U.S. had a decided preference for dealing among allies, "rather than through a multilateral arrangement with states that have different agendas and are less trusted."[8]

Continuous Monitoring substantially exacerbates the trust concerns. Highly time sensitive and trusted actionable information is constantly needed, and that is something which multilateral organizations are notoriously bad at. In organizations like the ITU, even relatively benign national telecommunication statistical information has been provided well after deadlines and regarded as so manipulated that it created secondary opportunities by third party companies and agencies to compile more trustworthy statistics.[9] Indeed, multilateral organizations are generally bound to accept provided information as fact and cannot independently question what they receive. Even where the multilateral organization might be providing the information based on some third parties, the organization may be introducing a further element of distrust by imposing itself in the middle.

Continuous Monitoring has arguably emerged as the principal viable approach for dealing with cyber security on a global scale.

The Flame Incident as a Multilateral Trust Challenge Example

On May 31, 2012, ITU Secretary-General Hamadoun Touré issued a press release announcing via a special relationship with the Russian cyber security firm Kaspersky Labs that the ITU was assisting the Iranian government with newly discovered malware dubbed "Flame," and that his office intended to play a leadership role to deal with new global cyber security threats.

Flame is a prime example of why governments and industry must work together to tackle cyber security at the global level. Early warning of new threats is vital and it is critical that best practice on required corrective steps is shared in order to best protect the global information society. This is the value in building a global coalition.[10]

What Touré apparently didn't know or wasn't told is that Flame was relatively common surveillance software that multiple cyber security organizations had been following and not a new massive global security challenge nor a threat to the "global information society."[11] Indeed, the day before the ICSCERT (Industrial Control Systems Computer Emergency Response Team) and the USCERT (United States Computer Emergency Readiness Team) released a joint advisory detailing its characteristics, explaining that it was designed to steal information, was confined, and described how to mitigate its propagation.[12]

The next day the *New York Times* published a front-page article based on anonymous high-level U.S. government sources, described a broad program of software based agents designed to support global actions for limiting nuclear weapons proliferation.[13] Although the details are not entirely known, it appears as if Flame may have been deployed by some governments to assess and watch for nuclear security threats. Subsequent press coverage and online discussion has continued to question the ITU actions in the matter and its role.[14]

Additional Impediments to Multilateral Solutions

CM is not the only factor that has an important effect on the use of multilateral solutions.

National borders are largely irrelevant and non-state actors abound in the cyber security realm. In fact, the non-state actor challenge worldwide has led to nations such

It is not realistic for large multilateral organizations to provide comparable capabilities because of need to coordinate resources among multiple nations in real time.

Cyber security technology is also dual use. Some of the same techniques that are used for cyber security can be used for surveillance of adversaries—both domestic and foreign—and are indeed marketed as such by vendors. The knowledge and expertise largely exists in the private sector and in a few state security communities. Large multilateral organizations have no effective means of compartmentalizing their information. As a result, no rational state is likely to dispose of its strategic advantages in these areas by making actionable information available to every other nation in the world through a multilateral organization.

Operational Network Security Roles Are Historically Difficult

As Sofaer-Clark-Diffie noted, there is no real multilateral body today in the field of information networks. Even in eras when the technology was less complex, multilateral organizations such as the ITU were unable to deal with relatively simple "cyber security" conflicts. Going back to the initial 1850 Dresden Convention on the Electrical Telegraph, a general escape clause was inserted that the signatories may avoid any specified treaty obligation when national security interests were at stake.

Over the years, when disputes did arise —for example, in the radio spectrum domain which is functionally an open global network similar to the Internet— the ability of the ITU to resolve disputes was usually not possible. Many states such as the U.S. refused categorically to accept any ITU dispute resolution jurisdiction.[15]

One particularly outstanding institutional example of a failed dispute resolution mechanism consisted of the International Frequency Registration Board, created in the spirit of multilateral idealism in the late 1940s. The Board barely got started before the Cold War began and the interest in its ability to perform a quasi-judicial role to resolve disputes over spectrum usage all but disappeared. For the past 50 years it has remained as essentially a dormant organ of the ITU.[16]

Useful Multilateral Organization Roles

There are significant roles to be exercised that have demonstrated value over many years and across multiple institutions. The most prominent and enduring of these value propositions are agreements on the technical formats and capabilities for exchanging cyber security information within diverse trust relationships. This approach is exemplified in ITU sector work, the Convention on Cybercrime, and a number of other multilateral cyber security activities today.

An example of multilateral cyber security activity that has provided global value, while avoiding counterproductive operational roles, has been ongoing in the ITU's technical standards body —the ITU-T— for the past three years. It has been successful in pulling together cyber security experts and bodies to assemble the specifications for techniques and activities intended to enhance trust and mitigate vulnerabilities. The activity involved almost constant, extensive "social networking" style collaboration with other groups where the real cyber security work has been ongoing among large numbers of companies and experts who participate in their own specialized forums.

These specifications dubbed CYBEX (Cyber Security Information Exchange) were published and continue to be advanced in the IETF (Internet Engineering Task Force), FIRST (Forum of Incident Response and Security Teams), and other bodies in collaboration with ITU-T which provides for broader outreach and consensus. They are based on actual specifications in use, and specifically include the most advanced current techniques for exchanging detailed technical information concerning Flame-like malware and other threats as well as their remediation. Continuous Monitoring is included. This work focused—as the name implies— on getting global agreement on "structured expressions" for exchanging in a coherent fashion, all manner of cyber security information and avoids duplicating specifications existing elsewhere.

Cyber security operations tend to be especially complex and sensitive as the actual exchange of the information inherently involves diverse compartmentalized trust communities who constantly collaborate among themselves.

The Cybercrime Convention is comprised of member states worldwide and has 47 signatories of which 35 have ratified. It establishes predicates for signatories in terms of their internal capabilities as well as contacts. The Council of Europe provides secretariat repository and other services. The Convention did not create an operational organization, but only the predicates for information exchange and trust relationships among its signatories.[17] Its signatories also meet annually and share views on global

research to assist potential signatories. The Convention has an expert and active secretariat. It helps get countries to agree to definitions of criminal cyber behavior and incorporate that and procedural law into their national laws.[18]

Additional examples of effective multilateral cooperation ensuing over the past several years include the establishment of the Common Criteria Recognition Agreement (CCRA) and its creation of the Common Criteria Development Board (CCDB) among more than 20 nations.[19] The Common Criteria is the driving force for the widest available mutual recognition of secure IT products. Recently, the CCDB has begun moving forward to promulgate and implement the Continuous Monitoring and SCAP suites.[20]

The NATO Consultation, Command and Control (C3) Agency has also been successful as a multilateral organization in moving forward with implementations among a broad ensemble of allies under the aegis of a Cyber Defense Data Exchange and Collaboration Infrastructure (CDXI).[21] The emphasis in NATO is generally oriented around assessing risk and managing trustworthiness. CDXI's special value is its ability to demonstrate how to successfully implement CM and share information within a strong multilateral security alliance among a diverse membership.

The European and Information Security Agency (ENISA) provides a mechanism for achieving cyber security solutions under the EU Treaty of Rome among member states. It has come to play an important role over the past two years in identifying institutions and exchanging related information similar to other multilateral endeavors.[22] Its focus includes European CERTs, CIIP and resilience, identity and trust, risk management, secure applications and services, and stakeholder relations. One of its important roles is to serve as a common means for coordinating the national CERTS within Europe.

The Forum of Incident Response and Security Teams (FIRST) is a private international organization that consists of many national governmental organizations dealing with incident response and remediation.[23] Strictly speaking, FIRST is not a multilateral organization but one that deserves status of "quasi-governmental" because of the extent to which governments are involved, as well as its uniqueness and extensive role in the cyber security arena. FIRST has also been given International Organization status by the ITU nation state members.

Notably, FIRST includes the National Computer Network Emergency Response Technical Team / Coordination Center of China (CNCERT/CC). The CNCERT plays the principal role within China in dealing with cyber security responses—particularly with external bodies—and hosts related expert workshops.

In addition to coordinating and facilitating responses to cyber threats and attacks among its different trust groups, FIRST maintains its own Special Interest Group standards forms for developing CM related standards. The Computer Vulnerability Scoring System (CVSS), for example, operates in conjunction with the Computer Vulnerabilities and Exposures (CVE) standard to enable the only global means for exchanging vulnerability information and assessing the associated risks. FIRST was created in 1989 and now consists of 260 teams across 55 countries.

What all of these multilateral activities in cyber security have in common is their focus on the technical formats and capabilities for exchanging information within diverse trust relationships. ■

Tony Rutkowski is a Distinguished Senior Research Fellow at the Georgia Institute of Technology's Center for International Strategy, Technology, and Policy (CISTP) at the Sam Nunn School of International Affairs.

William Abbott Foster is a Senior Research Associate at Georgia Tech's CISTP. Between 1995 and 2001, he was International Policy Editor or CIX, the world's first Internet Service Provider Association.

Seymour Goodman is Professor of International Affairs and Computing at the Sam Nunn School of International Affairs and the College of Computing, Georgia Institute of Technology. He also serves as Co-Director of both CISTP and the Georgia Tech Information Security Center (GTISC).

REFERENCES AND NOTES

[1] Tony Rutkowski is a Distinguished Senior Research Fellow at the Georgia Institute of Technology's Center for International Strategy, Technology, and Policy (CISTP) at the Sam Nunn School of International Affairs. As EVP for Yaana Technologies, he has served as rapporteur for cyber security at the ITU-T since 2009 and served as the counselor for two ITU Secretary-Generals between 1988 and 1992, co-authored a published ITU history, and led development and authored many cyber security standards and instruments as an engineer-lawyer over many years in multiple settings. See www.ngi.org. He can be reached at trutkowski@netmagic.com.

[2] William Abbott Foster is a Senior Research Associate at Georgia Tech's CISTP. Between 1995 and 2001, he was International Policy Editor or CIX, the world's first Internet Service Provider Association. He can be reached at Willam.Foster@inta.gatech.edu.

[3] Seymour Goodman is Professor of International Affairs and Computing at the Sam Nunn School of International Affairs and the College of Computing, Georgia Institute of Technology. He also serves as Co-Director of both CISTP and the Georgia Tech Information Security Center (GTISC). Immediately before moving to Georgia Tech in 2000 he was director of the Consortium for Research in Information Security and Policy (CRISP) at the Center for International Security and Cooperation, Stanford University. He can be reached at Seymour.Goodman@cc.gatech.edu.

[4] Abraham D. Sofaer, David Clark, and Whitfield Diffie, *Cyber Security and International Agreements* in Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, at 179-206, http://www.nap.edu/openbook.php?record_id=12997&page=179.

[5] See, e.g., ITU-T Rec. X.1205, Overview of Cyber Security (04/2008), https://www.itu.int/rec/T-REC-X.1205-200804-I

[6] See http://www.net-security.org/secworld.php?id=10333

[7] See NIST, Continuous Monitoring Workshop., http://scap.nist.gov/events/2011/cm_workshop/presentations/index.html. See especially, Continuous Monitoring Definition and Enterprise Architecture, Steve York, NSA. See also, NIST Continuous Monitoring FAQ, http://csrc.nist.gov/groups/SMA/fisma/documents/faq-continuous-monitoring.pdf; NIST Publishes Draft Implementation Guidance for Continuously Monitoring an Organization's IT System Security, https://www.itu.int/rec/T-REC-X.1205-200804-I.

[8] Ibid at 193.

[9] See, e.g., Telegraphy, http://www.telegeography.com ; CIA Factbook, https://www.itu.int/rec/T-REC-X.1205-200804-I

[10] See http://www.itu.int/net/pressoffice/press_releases/2012/34.aspx

[11] See http://en.wikipedia.org/wiki/Flame_(malware). See also, http://www.hackingteam.it/

[12] See http://www.us-cert.gov/control_systems/pdf/JSAR-12-151-01.pdf

[13] See http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?ref=stuxnet

[14] See http://www.nytimes.com/2012/06/04/technology/cyberweapon-warning-from-kaspersky-a-computer-security-expert.html?_r=1

[15] The instrument is known as the Optional Protocol on the Compulsory Settlement of Disputes Relating to the Constitution of the International Telecommunication Union, to the Convention of the International Telecommunication Union and to the Administrative Regulations Geneva, 1992. The accessions are reported in the Annual Report of the Activities of the ITU, Table IA.

[16] See the candid historical treatment on the ITU-R website at http://www.itu.int/ITU-R/information/promotion/e-flash/4/article7.html

[17] See Convention on Cybercrime and related materials at the COE secretariat, http://conventions.coe.int/Treaty/en/Treaties/html/185.htm, http://www.coe.int/what-we-do/rule-of-law/cybercrime

REFERENCES AND NOTES

[18] See http://www.coe.int/what-we-do/rule-of-law/cybercrime

[19] See Common Criteria Portal, http://www.commoncriteriaportal.org/

[20] See S. Barnum, Secure Content Automation Protocol (SCAP), MITRE, http://www.yourcreativesolutions.nl/ICCC12/p/110928/C02-Sean%20Barnum.pfd

[21] See Luc Dandurand, *Cyber Defence Data Exchange and Collaboration Infrastructure (CDXI)*, http://www.itu.int/dms_pub/itu-t/oth/06/35/T063500000200516PPTE.ppt; *Presentation to the ITU-T Cybex Working Group*, Cambridge, MA, 13 July 2011.

[22] See ENISA - Securing Europe's Information Society, http://www.enisa.europa.eu/

[23] See http://www.first.org