Explorations in Cyber International Relations Project
Science, Technology, & Public Policy Program

# NEW THREATS, OLD TECHNOLOGY

## VULNERABILITIES IN UNDERSEA COMMUNICATIONS CABLE NETWORK MANAGEMENT SYSTEMS

Michael Sechrist

HARVARD Kennedy School
Belfer Center for Science and International Affairs

February 2012

# NEW THREATS, OLD TECHNOLOGY

## VULNERABILITIES IN UNDERSEA COMMUNICATIONS CABLE NETWORK MANAGEMENT SYSTEMS

MICHAEL SECHRIST

HARVARD Kennedy School
BELFER CENTER for Science and International Affairs

FEBRUARY 2012

**Discussion Paper #2012-03**
**Science, Technology, & Public Policy Program Discussion Paper Series**

**Explorations in Cyber International Relations Project**
**Belfer Center for Science and International Affairs**
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138
Fax: (617) 495-8963
Email: belfer_center@harvard.edu
Website: http://belfercenter.org

This document appears as Discussion Paper #2012-03 of the Belfer Center Discussion Paper Series. Belfer Center Discussion Papers are works in progress. Comments are welcome and may be addressed to the author at michael_sechrist@hks.harvard.edu.

This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the Office of Naval Research.

Statements and views expressed in this discussion paper are solely those of the author and do not imply endorsement by Harvard University, the Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

## ACKNOWLEDGEMENTS

The author would like to thank Venky Narayanamurti, Laura Diaz-Anadon, Zachary Tumin, and the Harvard Kennedy School Information and Communication Technology Public Policy research fellows, specifically Lucas Kello and Vivek Mohan, for their helpful comments and support in editing this paper. Many thanks as well to James Smith, Susan Lynch, Patricia McLaughlin and Traci Farrell for their work all through the formatting and production process.

# ABSTRACT

Undersea cables are among the most critical technologies supporting today's global data and voice communications. Long-standing physical vulnerabilities to attack persist: cable landing stations, for example, cluster high-value cable systems at single geographic points, but without the physical protections provided to other critical infrastructure such as telecommunication data centers. With an increasing number of cable operators using remotely-controlled network management systems, operators have introduced additional risk of large-scale cyber attacks, adding new urgency to securing *all* potential points of compromise, both the physical sites and well as the logical infrastructure. While individually governments and industries have taken some steps to address such matters, much work remains. Collaboration on fortifying security with new regulatory and voluntary action, working through existing bodies such as Team Telecom under the Committee on Foreign Investment in the United States, and the International Cable Protection Committee, should accelerate.

# TABLE OF CONTENTS

# INTRODUCTION

Many cyber experts predict 2012 will usher in a new era of malware attacks on critical infrastructure systems. The predictions follow reports that the Stuxnet worm may have at least "four cousins," several of which have yet to be fully identified.[1]

Security firms now rank cyber attacks on industrial supervisory control and data acquisition ("SCADA") systems, which control everything from power to water, as among top threats. Surveying the field, McAfee concluded there was "little good news about cybersecurity [and] the crucial services that depend on information technology and industrial control systems."[2] Control systems, McAfee said, especially those connected to the Internet, introduce "significant vulnerabilities into systems never designed to sustain suck risks."[3]

Those vulnerabilities now proliferate. Conferees at January 2012's International Conference on Cyber Security heard reports of the discovery in 2011 of 147 so-called "zero-day vulnerabilities" – unpatched flaws – in Siemens-based SCADA systems.[4] In December 2011, the U.S. Department of Homeland security issued an alert: it had discovered "researchers" using a new search engine called "SHODAN". SHODAN's purpose: search and find Internet-facing control systems.[5]

The risk is real. In Texas, a hacker posted screen shots to the Internet of a SCADA system monitoring a water treatment plant in South Houston.[6] In late 2011, DHS Secretary Janet Napolitano said hackers have "come close" to shutting down elements of U.S. infrastructure,

[1] Jim Finkle, "Stuxnet Weapon Has At Least 4 Cousins: Researchers." Reuters, December 28, 2011. Accessed at http://www.msnbc.msn.com/id/45809884/ns/technology_and_science-security/t/stuxnet-weapon-has-least-cousins-researchers/#.TxTe05jkSS0
[2] Stewart Baker, Natalia Filipiak, and Katrina Timlin, "In the Dark: Crucial Industries Confront Cyber Attacks," McAfee, 2011. Accessed at https://portal.mcafee.com/downloads/General%20Documents/critical_infrastructure_report.pdf
[3] Angela Moscaritolo, "A 'Critical' Turning Point: The Nation's Critical Infrastructure." SC Magazine, January 3rd, 2012.
[4] Sara Yin, "Is Your SCADA Vulnerable to a Cyber Attack? Call 1-800-USA-0DAY," PC Magazine, January 11, 2012. Accessed at http://securitywatch.pcmag.com/none/292708-is-your-scada-vulnerable-to-a-cyber-attack-call-1-800-usa-0day
[5] ICS-CERT, "ICS-ALERT-11-343-01- Control System Internet Accessibility," December 9, 2011. Accessed here: http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-343-01.pdf
[6] Paul Roberts, "Was The Three Character Password Used To Hack South Houston's Water Treatment Plant A Siemens Default?," Threat Labs: Kaspersky Lab Security News Service, November 22, 2011. Accessed at http://threatpost.com/en_us/blogs/was-three-character-password-used-hack-south-houstons-water-treatment-plant-siemens-default-11

apparently both Wall Street and transportation systems.[7] Hackers compromised SCADA systems in three cities, the FBI reported, and could have "theoretically dumped sewage into a lake, or shut off the power to a shopping mall."[8]

With all the commotion, there exists now an abundance of regulation, advice – and confusion about what to do next. For all of the government's efforts, for example, the U.S. Government Accountability Office reported in 2012 that "DHS and the other sector-specific agencies have not identified the key cybersecurity guidance applicable to or widely used in each of their respective critical infrastructure sectors."[9]

This paper explores the vulnerabilities to cyber attacks of infrastructure that today carries nearly all the world's data and voice traffic: undersea communications cables. Long-standing physical vulnerabilities in cable infrastructure have been compounded by new risk found in the network management systems that monitor and control cable operations. Unlike an attack on a water treatment plant's control systems, however, an attack on the cables' control systems could devastate the world's economies – presenting a different kind of Internet "kill switch" altogether – shutting down world commerce, and doing it all with the click of a mouse.

[7] Ed O'Keefe, "Janet Napolitano: Hackers Have 'Come Close' To Major Cyberattack," The Washington Post, October 27, 2011. For further information on other critical infrastructure cyber attacks, please see Appendix B.

[8] Hal Hodson, "Hackers accessed city infrastructure via SCADA – FBI," Information Age, November 29, 2011. Accessed at http://www.information-age.com/channels/security-and-continuity/news/1676243/hackers-accessed-city-infrastructure-via-scada-fbi.thtml

[9] United States Government Accountability Office, "Cybersecurity Guidance Is Available, But More Can Be Done to Promote Its Use," GAO-12-92, Dec 9, 2011

# BRIEF BACKGROUND ON UNDERSEA COMMUNICATION CABLE SYSTEMS

Ever since the dot com bubble burst last decade, undersea communication cable operators have faced difficulties in generating a profitable business model. In the late 1990's and early 2000's, financial speculators invested heavily in building and deploying cables to accommodate the predicted Internet boom. When the bubble burst, global demand for bandwidth fell, creating significant bandwidth glut, primarily on U.S. trans-oceanic routes.[10]

As other industries have, undersea cable operators turned to technology to drive costs down and maintain profitability. Today, the undersea cable industry is finding better ways to connect itself over its own infrastructure. Network management systems, for example, help operators reduce personnel and management costs. Using remote, web-based technologies they connect cable systems, landing stations, spare depots, and other cable system components – all decreasing the need for humans in the equation.

Connecting cable sites with software creates more efficiency and provides operators greater operational awareness. However, it creates potential new risk, particularly to cyber attacks.

## CRITICALITY OF UNDERSEA CABLES

As a technology system with physical, logical, and human components, cables have long been a high-risk, single point of potential failure. For highly connected nations, both developing and developed, the consequence of failure is higher today than ever, as global Internet traffic has surged, and much of the world's commerce and security now relies on cable for nearly all its voice and data needs.

Undersea communication cables are, in fact, the *only* technology that can transmit large amounts of bandwidths across bodies of water at low latencies (delays) and low costs. In fact, undersea cable systems worldwide transmit nearly 99 percent of all trans-oceanic Internet and data traffic.[11] In the U.S., over 90 percent of international voice and data traffic is transmitted via fiber.[12]

[10] Stephan Beckert, "International Telecommunication Trends," PTC Conference Presentation, January 2011);
[11] Declan McCullagh, "NSA Eavesdropping: How It Might Work," ZDnet.com, February 7, 2006. Accessed at http://news.zdnet.com/2100-1009_22-146683.html
[12] Ibid.

Little can substitute for cable. In the event of a catastrophic failure to the entire cable architecture, for example, satellites and other technologies would likely be able to recoup only a sliver of that capacity.

With the world so dependent on cable systems, the technology needs to be among the most reliable in the world. Industry makes it so: cables are operational with up to "5 nines" reliability, or 99.999 percent of the time. Only highly critical systems such as space shuttle technology and nuclear weapons security have similar reliability.[13]

High reliability comes at high cost. Since undersea cable deployment is expensive, forces of history and economies of scale have, over time, concentrated cable landing sites in a few geographic areas. From GIS data, at least ten major cable chokepoints exist around the world today. For example, much of the U.S. trans-Atlantic bandwidth comes ashore in just a few locations within a 30-mile radius of New York City.[14] Some in the industry claim that nearly all that same trans-Atlantic traffic then funnels into one pipe under a single building in downtown Manhattan, contravening the popular belief of extraordinary redundancy and resiliency within today's telecommunications infrastructure.[15]

## CABLES AND THE FINANCIAL SERVICES INDUSTRY

With respect to global financial flows, in particular, undersea communication cables are exceptionally important.

- At a recent cable seminar, a U.S. Federal Reserve representative stated that cables carry an excess of $10 trillion a day in transactions.[16]
- The Society for Worldwide Interbank Financial Telecommunication (SWIFT) network uses undersea fiber-optic communications cables to transmit financial

[13] Karl Rauscher, Comments made at a ROGUCCI Seminar, New York City, November 10, 2011

[14] David Lloyd, "The Need For Physical Diversity For Submarine Cable Routing," Hibernia Atlantic website. October 2008. Accessed at http://www.hiberniaatlantic.com/documents/DaveysCorner-oct2008.pdf

[15] Michael Sechrist, "*Cyberspace in Deep Water: Protecting Undersea Communications Cables By Creating an International Public-Private Partnership," Harvard Kennedy School Policy Analysis Exercise, March* 2010. Page 21. Accessed at http://belfercenter.ksg.harvard.edu/publication/20710/cyberspace_in_deep_water.html?breadcrumb=%2Fexperts%2F2223%2Fmichael_sechrist

[16] Seminar panel held on the Reliability of Global Undersea Communications Cable Infrastructure, Goldman Sachs Headquarters, New York City, November 10, 2011

data to more than 8,300 member financial institutions in 195 countries.[17] In 2011, SWIFT's network handled nearly 15 million messages daily.

- The CLS Bank operates the largest multi-currency cash settlement system in the world, trading over 1 million transactions and over $4.7 trillion dollars a day over undersea cables.[18]
- The U.S. Clearing House Interbank Payment System processes over $1 trillion a day to more than 22 countries[19]

With trillions traded daily, a multi-cable outage, especially in a regional financial hub, has enormous ramifications for the global financial order. History proves this. One need only recall the days following the terrorist attacks of September 11, 2001, when one day later Wall Street was ready to trade, the Fed was eager to get capital flowing back into the markets – but the telecommunications infrastructure had succumbed to catastrophic failure. The global markets stood by, waiting.[20]

## CABLE LANDING SITES: EXPOSURES AND RISKS

While the financial services industry eventually moved to address this, there remain today numerous single points of physical risk: the places where cables make landfall, often clustered regionally.

The U.S. State Department listed the world's cable landing sites as among the most critical of infrastructures for the United States.[21] With good reason: by gaining access to terminals located within cable landing sites, or to control systems managing the fiber-optic wavelengths themselves, a hacker could acquire control over portions of international data and voice traffic and, potentially, the power to disrupt or degrade significant portions of states' cyber infrastructure.

[17] Douglas Burnett, "Cable Vision," 2011 Proceedings, U.S. Naval Institute. Accessed at www.usni.org

[18] Ibid.

[19] Burnett, Cable Vision.

[20] Detailed in the section, "Waiting for Verizon," in William Bratton and Zachary Tumin, *Collaborate or Perish! Reaching Across Boundaries in a Networked World.* New York: Random House. 2012.

[21] Mark Clayton, "WikiLeaks List of 'Critical' Sites: Is It a 'Menu for Terrorists'?," The Christian Science Monitor, December 6, 2010. Accessed at http://www.csmonitor.com/USA/Foreign-Policy/2010/1206/WikiLeaks-list-of-critical-sites-Is-it-a-menu-for-terrorists

That capability is prized by defense and intelligence agencies the world over. Nor are governments alone: cyber criminals, hackers, terrorists and other non-state actors are determined to acquire this capability.

With the risk of attack and the cost of compromise high, it is critical that industry and government treat cable system physical security and access with the utmost seriousness and concern – even to the same “five nines” they accord other critical infrastructure, like nuclear power plants. To date, however, that has not occurred.

# ENTER UNDERSEA CABLE NETWORK MANAGEMENT SYSTEMS

With old physical risks unaddressed and exacerbated by new, massive global reliance on cable-borne data traffic, new logical risks to the undersea cable infrastructure have emerged to make matters worse. That new logical risk comes from the very network management systems ("NMS") that operators have installed to manage their operations efficiently.

NMS are not new. Vendors have marketed NMS in various forms since at least the early 1990's. Nonetheless, today's versions are much more comprehensive than their predecessors, and more mainstream – and scarier.

## NEW CAPABILITIES, NEW WORRIES

Network managements systems are offered by several firms, including the three major undersea cable layer-operators -- TE Subcom, NEC, and Alcatel-Lucent. In general, NMS gives operators centralized control over the cable network, its individual parts (or elements), and access to all via web-based platforms.

Using its NMS, for example, operators can manage field elements of an undersea communication cable system from anywhere in the world. This includes the cables' physical and optical layer, line terminal equipment, repeaters, branching units, landing stations and other network operation centers, even those residing in other nations.

Today's NMS have potent capabilities. For example, they allow for Reconfigurable Optical Add/Drop Multiplexing ("ROADM"). ROADM allows users to activate or remove optical wavelengths from a selected cable system. Using ROADM a system user could, for example, delete "the blue wavelength on channel 32" from a particular cable system. That wavelength might transmit all communications from Internet addresses belonging to a small country - like Yemen, Bahrain, or Estonia - to that landing site.

Using ROADM, a user could remove *all* wavelengths on a particular cable, effectively shutting down large portions of data traffic for multiple states. And using its NMS, an operator can monitor wavelengths for "loss of light" situations due to faults, engineering malfunctions, or disruptions. But a hacker could direct a system to show the operator system condition "green", when actually the system is blinking red. The consequence: an unauthorized user could siphon off wavelengths or create temporary disruptions without the operator knowing.

## NEW SYSTEMS, OLD VULNERABILITIES

Within these systems, numerous cyber security concerns exist. Today, for example, NMS typically rely on HTTP, TCP/IP, Windows operating systems and web browsers like Microsoft Internet Explorer to connect to network operations centers and cable system field elements. It is reportedly "common practice to connect critical infrastructure systems to the Internet and then manage them with commonly available software."[22]

It is also worrisome. Any system with web capabilities is an easier target for hackers than one that lacks them. The exploitable aspects of HTTP, Windows OS and Microsoft IE are, in fact, significant and well understood by cyber security experts.

Not only are most NMS applications web-based, they are designed for computers running on Microsoft operating systems. Microsoft operating systems in particular are among the most attacked operating systems in the world[23].

The risk to NMS and to cable operations therefore multiplies when the NMS "brain" – its supervisory control and data acquisition (SCADA) system - both runs Windows operating systems, and is connected to the Internet. Attackers can easily access and use Stuxnet-like code to attack most SCADA systems, particularly those based on legacy Siemens' equipment. Two Windows applications exploits in particular reportedly still exist - one aimed at Siemens Simatic Manager and WinCC SCADA application; the other at Siemens S70-300 and 400 series controllers.[24]

What is the nightmare scenario? A hacker penetrates a cable management system, gains administrative rights, and hacks into the presentation server. Presentation servers can host web-based applications for numerous cable operators and handle management system data for multiple cable systems. Hacking into a presentation server can therefore provide attackers with access to control of multiple cable management systems. Hackers could then attain unprecedented top-level views of multiple cable networks and data flows, discover physical cable vulnerabilities, and disrupt and divert data traffic. With that access, hackers/attackers can gain a potential "kill

[22] McAfee Labs, 2012 Threat Predictions, accessed at http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf

[23] Trend Micro, "3rd Quarter Quarterly Roundup," November 2011. Page 5. Accessed at http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/3q_2011_threat_roundup.pdf

[24] Paul Roberts, "Many Stuxnet Vulnerabilities Still Unpatched," ThreatPost: Kaspersky Lab Security News Service, June 8, 2011. Accessed at http://threatpost.com/en_us/blogs/many-stuxnet-vulnerabilities-still-unpatched-060811

click" – with a click of a mouse they can delete wavelengths and, potentially, significantly disrupt or alter global Internet traffic routes.

## NEW SYSTEMS, NEW VULNERABILITIES?

In March 2011, Nokia Siemens demonstrated its new undersea line terminal equipment, the hiT 7300 platform. The Nokia Siemens NMS makes life easy for the customers. With it they have "remote network termination" capability, and "remote access [with] no system-specific know-how or laptop required for any on-site installation, commissioning, provisioning."[25]

Experts warn that Siemens equipment, new or legacy, should give cable operators pause. Although Siemens has reportedly been at work repairing its compromised technology,[26] it is unclear whether new Siemens-enabled products contain any of the control systems compromised in the Stuxnet attack. If they do, as recent reports suggest they might[27], that could be a concern. Ralph Langner, the expert who decoded the Stuxnet worm, recently asserted that Stuxnet can easily be downloaded and copied into new forms of attacks on SCADA systems. "Siemens customers," cautioned Langner, "should be very concerned about attacks." [28]

Cable operators may be left with few good choices. Only one major undersea cable provider, for example, boasts of offering secure, integrated management software: Huawei Marine Networks. Uniquely among NMS providers, Huawei's NMS claims use of HTTPS/SSL. It provides "optional" access control tools and security tools to prevent hacking, viruses, and worms. [29]

If true, such protections may provide Huawei with first-mover advantage among cable operators in offering secure NMS. That is worrisome for the United States and its allies – particularly the defense and intelligence communities. [30] U.S. officials believe that former Peoples' Liberations

[25] Nokia Siemens hiT 7300 Product Overview. Accessed at http://www.nokiasiemensnetworks.com/portfolio/products/transport-networks/optical-transport/hit-7300

[26] Paul Roberts, "Siemens Working on Fixing Security Gap in Logic Controllers," ThreatPost: Kaspersky Lab Security News Service, May 24, 2011. Accessed at http://threatpost.com/en_us/blogs/siemens-working-fix-security-gaps-logic-controllers-052411

[27] Paul Roberts, "Update: Looking for a Firesheep, researchers lay bare woeful SCADA security," January 20, 2012. Accessed at http://threatpost.com/en_us/blogs/looking-firesheep-moment-researchers-lay-bare-woeful-scada-security-012012?utm_source=Threatpost&utm_medium=Tabs&utm_campaign=Today%27s+Most+Popular

[28] Roberts, *op cit.*

[29] Ibid.

[30] US-China Economic and Security Review Commission (USCC), "The National Security Implications of Investment and Products from the People's Republic of China in the Telecommunications Sector," January 2011

Army (PLA) officials with direct connections to the Chinese military establishment run Huawei. The company and its products are matters of ongoing concern, and for the most part are not approved for use by any U.S. company, particularly companies operating critical or sensitive infrastructure.[31]

## SUMMING UP: OLD PROBLEMS, NEW VULNERABILITIES

Poor physical security of cable landing sites is a potential Achilles heel for U.S. and global cyber security. Cable landing sites have always been and continue to be single points of potentially catastrophic attack and failure that must be addressed.

Today, however, risk to global safety and security is compounded by the vulnerability of cable systems to cyber attacks through new network management systems. These attacks can gain access to systems by exploiting physical vulnerabilities like those at cable landing sites, as well as by Internet-based vulnerabilities.

With global commerce and security now nearly entirely dependent upon the security of this physical and logical infrastructure, the consequences of such failure could be devastating. A decade ago, former Secretary of State Condoleezza Rice stated, "The cyber economy is the economy. Corrupt those networks and you disrupt this nation."[32] Corrupting cable network management systems is surely a significant way to disrupt our national economy. Renewed attention to both physical and logical security is urgently required.

[31] Claude Barfield, "Telecoms and the Huawei conundrum: Chinese foreign direct investment in the United States." American Enterprise Institute Economic Studies, November 16, 2011. Accessed at http://www.aei.org/files/2011/11/21/-telecoms-and-the-huawei-conundrum-chinese-foreign-direct-investment-in-the-united-states_170712239630.pdf
[32] Condoleezza Rice, "Remarks to the Partnership for Critical Infrastructure," U.S. Chamber of Commerce," March 23, 2001, accessed at http://www.house.gov/jec/security.pdf

# A PROBLEM IN NEED OF A RESPONSE: DOMESTIC POLICY CONSIDERATIONS

Today, the Committee on Foreign Investment in the United States (CFIUS), an inter-agency group chaired by the United States Treasury, has a direct role in reviewing all applications for cable landing licenses. Through a CFIUS subgroup, dubbed "Team Telecom," the U.S. reviews all undersea cable landing license applications for national security purposes. Ultimately, the Federal Communications Commission receives and must approve all such applications. The FCC refers all applications to Team Telecom for prior review. Applicants must clear Team Telecom's national security review before the FCC will consider granting a cable landing license.[33] [34]

Team Telecom is therefore one of the most important gatekeepers in the U.S. regulatory scheme established to address the national security requirements for cable systems. As the U.S. government considers whether additional regulations might be required, Team Telecom could be the appropriate body to implement policies to minimize cyber security risks to cable systems.

For starters, Team Telecom could mandate that cable operators use secure management systems, or use them only with significant encryption/security protocols in place. Team Telecom should also ensure that computers operating cable management system software be patched continuously with the latest cybersecurity fixes in order to avoid glaring gaps.

The group could require cable operators who use management systems to immediately upgrade security software in line with the most advanced security protections afforded to other critical national infrastructure systems. High-security SCADA systems are on the market. For instance, one company recently launched an "ultra secure 3rd generation networked SCADA system," which uses a "mutual authentication system to verify the remote management server and the controller to each other before allowing the software to be upgraded on the remote SCADA device."[35] Such systems seek to stem the rising SCADA vulnerabilities by protecting it from

[33] Kent Bressie, "More Unwritten Rules: Developments in U.S. National Security Regulation of Undersea Cable Systems," Presentation to the 2009 PTC conference, January 18, 2009. Accessed at http://www.harriswiltshire.com/siteFiles/News/7DF1C8D035660E8FBEF0AAC7BA8DA103.pdf

[34] Kent Bressie, "New Barriers to U.S. Market Entry for Undersea Cable Operators: Recent Developments with 'Team Telecom'," Presentation to the 2008 PTC conference, January 13, 2008. Accessed at www.ptc.org/ptc08/participants/speakers/papers/BressieFinalSlides.pdf

[35] "Cambridge company Launches Ultra-Secure 3rd Generation Networked SCADA System," Darkreading.com, January 17, 2012. Accessed at http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/232400480/cambridge-company-launches-ultra-secure-3rd-generation-networked-scada-system.html

locally installed malware and securing the connection at all times.

Further, Team Telecom could require cable operators to consider removing access to the ROADM portion of these systems, or increase security measures in order to get to them on management systems.  Air gapping computers that are allowed to add/drop wavelengths from the Internet might be one cost effective way to safeguard that aspect.

It might also be prudent for the U.S. government to provide some sort of financial incentives for companies to help reduce the costs associated with improving network management system security.  As a direct incentive, the U.S. Department of Homeland Security could provide monetary grants to the cable companies offering these products.  As an indirect incentive, the U.S. Federal Communications Commission might be able to decrease the initial permitting costs cable operators pay to land a system on U.S. soil.

## GLOBAL COLLABORATION FOR CABLE SECURITY

Cable architecture spans the globe and acts as the arteries of the global digital infrastructure.  No one nation or company can truly ensure high-level security, unless all are committed to doing so. This interdependence is one reason why cybersecurity problems are so frustratingly complex and difficult to solve; the solution resides in near seamless state and non-state actor collaboration.

The International Cable Protection Committee (ICPC) might provide a good venue to enact global security changes to management system software.  About one hundred and twenty-five cable industry companies comprise the ICPC.

Last year, the ICPC opened its membership to nation states.  So far, Australia and Singapore have joined.  With nation states joining, perhaps the time is right for ICPC to create an international norm in this area and recognize the threat cyber attacks pose to these systems.  Today, the ICPC can recommend that its members' implement secure management systems around the world. Tomorrow, members could be encouraged to sign a public, voluntary pledge to limit the spread of such attacks and the group could devote some measure of resources to ensuring those that take the pledge actually implement it.   In this way, the ICPC leadership might use some of those resources to provide an external audit function to certify members' use of secure software.

# APPENDIX A: A PROFILE OF CYBER VULNERABILITIES IN THREE MAJOR MANAGEMENT SYSTEMS

**PROFILE: NEC's WebNSV UMS/EMS**[36]

- The NEC system controls multiple landing stations, such as the per-wavelength management of OADM branching units (BUs) and the switching of power feed paths, as well as the monitoring of faults over the entire system.
- The EMS … is highly extendible for monitoring up to 1,000 network elements (NE), including the LTE (Line Terminal Equipment), PFE (Power Feeding Equipment) and RFTE (Remote Fiber Testing Equipment)
- Systems accessed on PC via web-based system with single sign-on authorization (i.e. username and password)
- "All components are written in Java and communicate through Remote Method Invocation protocol (RMI) whilst eXtended Markup Language XML is used for configuration."
- The EMS and UMS are connected via the inter-station data communication network (DCN) using Transmission Control Protocol/Internet Protocol (TCP/IP). The UMS also adopts a server/client configuration as do the EMS and runs Java programs. The server uses Linux as the operating system (OS) while the client's OS supports Microsoft Windows.
- Encryption protocols between server and computer is currently "optional"
- All landing stations, even those unattended, can be monitored remotely from one location.

[36] Information on the NEC WebNSV UMS/EMS was collected from two conference reports presented at the 2010 SubOptic Conference: Ken-ichi Nomura, "NEC's Unified and Element Management System for an Advanced Undersea Cable Network," SubOptic 2010 Poster Session, May 2010. Accessed at http://suboptic.org/App/Uploads/Files/Poster%20257%20Kenichi%20Nomura.pdf
Ken-ichi Nomura, Yasuhiro Aoki, Taka-aki Takeda, "Unified & Element Management System for Advanced Undersea Cable Network," SubOptic 2010 conference paper, May 12, 2010. Accessed at http://suboptic.org/App/Uploads/Files/257_Poster_EC_05.pdf

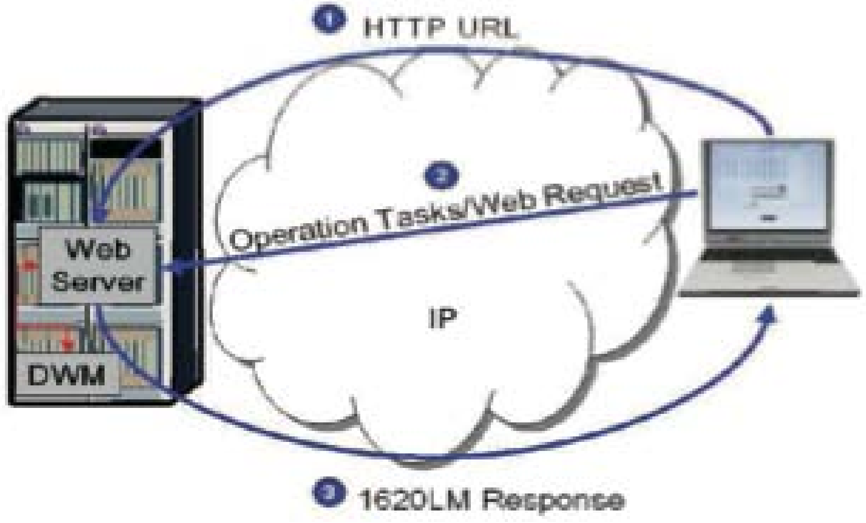
**PROFILE: Alcatel-Lucent's 1350 Optical Management System (OMS)**[37]

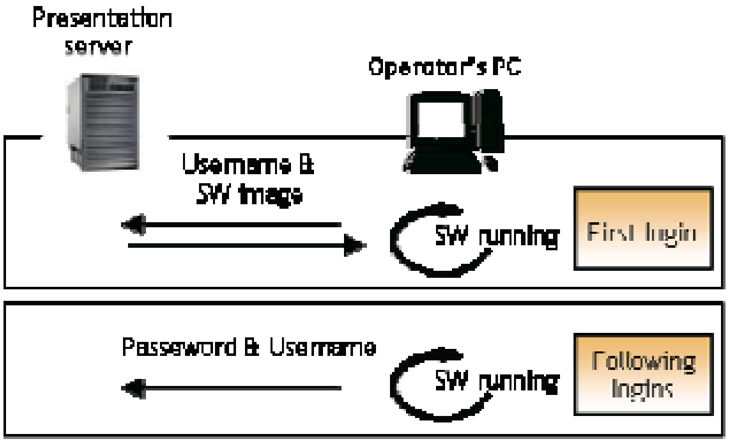
- The 1350 OMS provides the capability to start and stop applications independently, and is available in compact or distributed configurations.
- Uses a common desktop, login and security; common GUI and maps; common fault management; and common PM.
- This architecture allows Alcatel- Lucent to provide a single system with single integration points for multiple optical network technologies and all network sizes.
- Equivalent technology-specific solutions would require four or five separate systems.
- Self-service supervision and control: where the network operator provides end-user self-serve facilities (to check own service connections; optionally to also setup/clear down).

Graphical depictions of Alcatel-Lucent's system, collected from the SubOptic conference paper, are found below. Note the web-based system is accessible via an HTTP URL with a single sign-on username and password, where it then connects to a presentation server. These servers can host information related to several, unrelated cable systems.

[37] Information on Alcatel-Lucent's 1350 OMS was collected from several documents:
See "Alcatel-Lucent 1350 OMS Optical Management System," Alcatel-Lucent Company Brochure. Accessed at http://www.alcatel-lucent.com/wps/DocumentStreamerServlet?LMSG_CABINET=LGS_Resources&LMSG_CONTENT_FILE=Brochures/1350_OMS_R9-1_bro.pdf&lu_lang_code=en_WW,
"Alcatel-Lucent 1350 Management Suite," Alcatel-Lucent website. Accessed at http://www.alcatel-lucent.com/wps/portal/!ut/p/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLd4w3MfQFSYGYRq6m-pEoYgbxjgiRIH1vfV-P_NxU_QD9gtzQiHJHR0UAAD_zXg!!/delta/base64xml/L0lJayEvUUd3QndJQSEvNElVRkNBISEvNl9BXzNBRC9lbl93dw!!?LMSG_CABINET=Solution_Product_Catalog&LMSG_CONTENT_FILE=Products/Product_Detail_000328.xml#tabAnchor3
Richard Cruau, "Web Based Undersea Management Solutions," SubOptic 2010 conference paper, May 2010. Accessed at http://suboptic.org/App/Uploads/Files/314_Poster_EC_11.pdf

**Graphical Representation of Alcatel-Lucent's 1350 OMS**





(Source: Cruau, SubOptic 2010)

**PROFILE: TE SubComs' Network Management System (TEMS-NMS)**[38]

- TEMS-NMS is "implemented primarily using C++ and Java programming languages"
- "…Executes on the Linux operating system using commercial off the shelf (COTS) hardware"
- "…A customer may access TEMS-NMS using Virtual Network Computing (VNC) technology which is supported in common environments such as Microsoft Windows5 with the Microsoft Internet Explorer6 browser."[39]
- "Manages current & historical information"
- "Auto-Discovery & Manual Updates"
- "Secure web user accessibility" (presumably the username/password)
- "Automatic & Manual state changes"

[38] Information on the TEMS-NMS was collected from two SubOptic 2010 conference reports: Ricardo Alves, Glen Goto, Richard Kram, Jonathan Liss, Sameh Sabet, Meir Winston, "A Distributed & Integrated Inventory Management Capability for Network Management Systems," SubOptic 2010 Poster Presentation, May 2010. Accessed at http://suboptic.org/App/Uploads/Files/Poster%20325%20Jonathan%20Liss.pdf

[39] Jonathan Liss, Renata Bodner, Sameh Sabet and Ricardo Alves, " A Next Generation Distributed Network Management System," SubOptic 2007 Conference Paper, May 2007. Accessed at http://suboptic.org/App/Uploads/Files/We3.02.pdf

# APPENDIX B: OTHER CRITICAL INFRASTRUCTURE ATTACKS

Before Stuxnet, cyber attacks on critical infrastructure were thought-experiments, at least in the U.S. Malware had infected critical infrastructure assets before most notably in the 2008 crash of Spanair flight 5022 and energy blackouts in Brazil in 2005 and 2007.

In the Spanair flight crash, [investigators] "discovered a central computer system used to monitor technical problems in the aircraft was infected with malware. An internal report issued by the airline revealed the infected computer failed to detect three technical problems with the aircraft, which if detected, may have prevented the plane from taking off, according to reports in the Spanish newspaper, El Pais."[40]

In 2010, several U.S. intelligence sources confirmed to CBS News that there were a series of cyber attacks in Brazil: one north of Rio de Janeiro in January 2005 that affected three cities and tens of thousands of people, and another, much larger event beginning on Sept. 26, 2007. The 2007 blackout "in the state of Espirito Santo affected more than three million people in dozens of cities over a two-day period, causing major disruptions. In Vitoria, the world's largest iron ore producer had seven plants knocked offline, costing the company $7 million. It is not clear who did it or what the motive was."[41]

Symantec also recently confirmed that a new worm, W32.Duqu, is a threat nearly identical to Stuxnet, but with a completely different purpose. Duqu "was written by the same authors…[whose] purpose is to gather intelligence data and assets from entities such as industrial infrastructure and system manufacturers, amongst others not in the industrial sector, in order to more easily conduct a future attack against another third party."[42]

There have been others and there will be more.

These capabilities create a significant new logical security risk, made worse by the exposure of the physical infrastructure. Given the importance of undersea cables to the global Internet

[40] Leslie Meredith, "Malware implicated in fatal Spanair plane crash," MSNBC.com, August 20, 2010. Accessed at http://www.msnbc.msn.com/id/38790670/ns/technology_and_science-security/#.TtlGM1awVid

[41] "Cyber War: Sabotaging the System," CBS News, June 15, 2010. Accessed at http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml

[42] W32.Duqu: The precursor to the next Stuxnet, Symantec, November 23, 2011. Accessed at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

infrastructure, it is clear that any system must provide both *physical* security for its infrastructure and *logical* security within its management systems.

The failure to secure portions of undersea cable infrastructure, including fiber-optic lines and field element units, now means that the majority of cable landing sites and associated NOCs may be exposed to cyber attacks, even rudimentary ones, via their powerful network management systems.

Ralph also argues that the U.S. is not doing enough to protect critical infrastructure from copycat Stuxnet attacks. "Most engineers are aware of the problem, it's just that they don't get the budget to fix the problem. The risk is just discounted. As long as management doesn't see an immediate threat, there is a tendency to ignore it because it costs money to fix," he stated[43]

The lack of a security budget parallels the situation in the undersea cable industry.

[43] Mark Clayton, "From the man who discovered Stuxnet, dire warnings one year later," Christian Science Monitor, September 21, 2011. Accessed at http://www.csmonitor.com/USA/2011/0922/From-the-man-who-discovered-Stuxnet-dire-warnings-one-year-later/(page)/2

**Belfer Center for Science and International Affairs**
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138
Fax: (617) 495-8963
Email: belfer_center@harvard.edu
Website: http://belfercenter.org