



## ICSJWG Quarterly Newsletter

### ICSJWG 2010 Fall Conference

In October, over 250 control systems professionals from government, industry, and academia gathered for two days at the Industrial Control Systems Joint Working Group (ICSJWG) 2010 Fall Conference in Seattle, Washington. Leading ICS security experts presented a wide variety of ICS security topics of interest to the control systems community, including standards, security solutions, and recent research results.

Due to the recent news coverage of the Stuxnet worm, this topic became one of the main themes for discussion during the conference. A two-hour time slot was dedicated for a panel of presenters from ICS-CERT, Microsoft, Industrial Defender, and North American Electric Reliability Corporation (NERC) to talk about the history, capabilities, and intent of the Stuxnet worm; its implications on the present and future state of control systems security; effectiveness of the ICS security regulations and technologies against such a sophisticated threat; and the findings and recommendations made by the newly formed NERC tiger team. The emergence of Stuxnet also underscores the importance for malware detection and prevention tools. Following the Stuxnet panel presentations, a Tools and Remediation Hands-on Workshop allowed attendees to receive demonstrations of various remediation tools.

Representatives from ICS-CERT and the Volpe National Transportation Systems Center travelled to the conference to discuss what their organizations can do to support both government and industry organizations. Julio Rodriguez gave a briefing on ICS-CERT's role, activities, major milestones, and products, and David Sawin discussed the roles and responsibilities of the Volpe Center in its support of the DHS Control Systems Security Program (CSSP).

In addition to the presentations, several of the ICSJWG subgroups had an opportunity to meet face-to-face and collaborate on their respective deliverables the day before the official kick-off of the conference. Members of the Roadmap, Research and Development, Vendor, and Workforce Development subgroups convened to discuss the status of their goals and objectives and

### About the ICSJWG

*The ICSJWG is a collaborative and coordinating body operating under the Critical Infrastructure Partnership Advisory Council (CIPAC) requirements. The ICSJWG provides a vehicle for communicating and partnering across all critical infrastructure and key resources (CIKR) sectors between federal agencies and departments as well as private asset owner/operators of industrial control systems. The goal of the ICSJWG is to continue and enhance the facilitation and collaboration of the industrial control systems stakeholder community in securing CIKR by accelerating the design, development, and deployment of secure industrial control systems.*

For more information, visit [http://www.us-cert.gov/control\\_systems/icsjwg/](http://www.us-cert.gov/control_systems/icsjwg/)

### Table of Contents

- ICSJWG 2010 Fall Conference ..... 1
- ICSJWG Subgroup Status..... 2
- Homeland Security Information Network (HSIN)..... 4
- Advanced Training Events Scheduled for 2011 ..... 4
- Industrial Control Systems Articles ..... 5
  - ISASecure Embedded Device Security Assurance (EDSA) Certification Program Is Operational..... 5
  - Cyber Security, Providing Value Through a Collaborative Team Approach ..... 7
  - A New Cold War? ..... 11
  - Participation is Key!..... 13
  - CSSP Contact Information ..... 13

the way forward. The ICSJWG received positive feedback about this session and is planning to continue with the face-to-face meetings for the 2011 Spring conference. Many of the attendees felt this was the best conference to date.

Presentations from the ICSJWG Fall 2010 Conference are posted at [http://www.us-cert.gov/control\\_systems/icsjwg/presentations.html](http://www.us-cert.gov/control_systems/icsjwg/presentations.html) as well as on HSIN: <https://cs.hsin.gov/C10/C1/ICSJWG/Lists/Announcements/DispForm.aspx?ID=17&Source=https%3A%2F%2Fcs.hsin.gov%2FC10%2FC1%2FICSJWG%2Fdefault%2Easpx> .

The ICSJWG is tentatively planning its next conference for May 3-4, 2011, in Chicago, Illinois, with subgroup face-to-face meetings on May 2nd and control systems security training on May 5th. More information on the venue, speaker abstract due dates and other details will be distributed in the near future.

---

## **ICSJWG Subgroup Status**

Below is an update on the progress of the ICSJWG subgroups. If you would like to become a member in any of the subgroups, send an email with your contact information to: [icsjwg@dhs.gov](mailto:icsjwg@dhs.gov) or contact the co-chairs directly.

### ➤ **Roadmap to Secure Industrial Control Systems Subgroup**

*GCC Co-Chair: Perry Pederson ([perry.pederson@nrc.gov](mailto:perry.pederson@nrc.gov))*

*SCC Co-Chair: Tim Roxey ([Tim.Roxey@nrc.net](mailto:Tim.Roxey@nrc.net))*

The Roadmap subgroup had great turnout at the Fall 2010 conference working meeting where members adjudicated the remaining comments that were received on the draft *Cross-Sector Roadmap to Secure Control Systems*. The subgroup members are currently meeting monthly to finalize the Roadmap, with the final document scheduled to be published in Spring 2011. In addition, the subgroup members are finalizing a business case methodology that can be used by organizations who wish to adopt the strategies outlined in the Roadmap. The subgroup reached a consensus to extend the charter to provide periodic updates to the Roadmap document.

### ➤ **Vendor Subgroup**

*GCC Co-Chair: Rick Lichtenfels ([cssp@dhs.gov](mailto:cssp@dhs.gov))*

*SCC Co-Chair: Eric Cosman ([ECCosman@dow.com](mailto:ECCosman@dow.com))*

The Vendor subgroup is in the process of putting together a *Vulnerability Disclosure Framework* document. The focus of this document is to help vendors understand general practices for disclosing vulnerabilities and to outline a realistic vulnerability disclosure framework that takes into account both vendors' and the government's needs. Once a draft is finalized, it will be posted on HSIN for review

The subgroup sees itself as a resource for other subgroups, providing the voice/position of the vendor community. During the Fall conference, members of this subgroup volunteered to be "ambassadors" to each of the other subgroups. Members will be reaching out to the other subgroups and attend their meetings.

- R&D – Kevin Staggs & Markus Braendle
- International – Art Manion & Marcus Braendle
- Information Sharing – Art Manion & Walt Sikora
- Roadmap – Rob McComber & Ernie Rakaczky
- Workforce Development – Bryan Owen

➤ **Workforce Development Subgroup**

*GCC Co-Chair: Dr. John Saunders ([saunders@ndu.edu](mailto:saunders@ndu.edu))*

*SCC Co-Chair: VACANT*

The Workforce Development Subgroup is still tackling their deliverables. If you have any experience in the ICS workforce development area or would like to volunteer with this group, please contact [ICSWJG@dhs.gov](mailto:ICSWJG@dhs.gov).

One of the GCC Co-chairs, Ben Wible, and the SCC co-chair, Marcus Sachs, both resigned from their positions due to other responsibilities. If you or anyone you know would be interested in these positions, please email Jeff Gray at [Jeff.Gray@hq.dhs.gov](mailto:Jeff.Gray@hq.dhs.gov) for more information on the responsibilities for this position.

➤ **Research and Development Subgroup**

*GCC Co-Chair: Dr. Douglas Maughan ([Douglas.Maughan@dhs.gov](mailto:Douglas.Maughan@dhs.gov))*

*SCC Co-Chair: David L Norton ([DNORTOI@entergy.com](mailto:DNORTOI@entergy.com))*

The Research & Development subgroup continues to focus on objective #1 in their charter, which is to identify existing and planned R&D needs and priorities as they relate to ICS. The group had a large meeting during the Fall conference and made significant progress on how they want to move forward in the future. The group is also looking to increase its membership and to work on developing a relationship with the Vendor community.

➤ **International Subgroup**

*GCC Co-Chair: Seán McGurk ([cssp@dhs.gov](mailto:cssp@dhs.gov))*

*SCC Co-Chair: Graham Speake ([graham.speake@us.yokogawa.com](mailto:graham.speake@us.yokogawa.com))*

The International subgroup will continue as a registration point for ICS professionals and will exist as a venue for remaining informed as to activities of the ICSJWG community. While no actual meetings are currently planned, the International membership will be informed of all ICSJWG news and be welcomed to events.

➤ **Information Sharing Subgroup**

*GCC Co-Chair: George Bamford*

*SCC Co-Chair: VACANT*

The ICSJWG Information Sharing subgroup is currently on hold subsequent to the launch of the HSIN portal.

## ***Homeland Security Information Network (HSIN)***

HSIN is now fully developed and in use by ICSJWG subgroup members. Subgroup members can keep abreast of upcoming meetings through the calendars in HSIN. The “Alert Me” feature can keep users up to date with changes to the portal. Alert results can be sent immediately, daily, or weekly. To sign up for alerts, click on the “Alert Me” link on the left-hand side of the ICSJWG home page and choose your delivery option.

If you are a subgroup member, please add your contact information under the Contacts List for each respective subgroup in which you are a member so that other people in the subgroup can contact you.

ICSJWG subgroup members who still need access to HSIN may send an email to [icsjwg@dhs.gov](mailto:icsjwg@dhs.gov) to request an account.

- **If you do not currently have a HSIN account**, please provide your name, company, contact information, critical infrastructure sector, and ICSJWG subgroup affiliations.
- **If you already have an HSIN account**, please provide your name, HSIN user name, ICSJWG subgroup affiliation, and critical infrastructure sector.

At this time DHS is not able to grant International members access to the HSIN portal. The owners of the HSIN Portal are reviewing sharing agreements of information posted to the site. Until that process is complete, the granting of International user accounts will be on hold. ICSJWG Communications will contact all International members immediately once a solution is in place or if there is additional information.

---

## ***Advanced Training Events Scheduled for 2011***

CSSP is currently offering advanced cyber security training sessions at the Control Systems Analysis Center located in Idaho Falls, Idaho. These sessions will provide intensive hands-on training on protecting and securing control systems from cyber attacks, including a very realistic Red Team / Blue Team exercise that will be conducted within an actual control systems environment. It will also provide attendees with an opportunity to network and collaborate with other colleagues involved in operating and protecting control systems networks.

The following advanced training events have been scheduled for 2011:

- **February 14-18, 2011:** Industry
- **March 14-18, 2011:** Industry
- **May 9-13, 2011:** International Partners
- **June 6-10, 2011:** All Applicants
- **June 20-24, 2011:** Industry
- **July 18-22, 2011:** Industry
- **September 12-16, 2011:** International Partners
- **October 10-14, 2011:** Industry
- **November 7-11, 2011:** Reserved
- **December 5-9, 2011:** Industry

There is no cost to attend the training; however, travel expenses and accommodations are the responsibility of each participant.

Additional offerings are being planned and will be announced once dates are finalized. More information, including registration and future offerings, is available at: [http://www.us-cert.gov/control\\_systems/cstraining.html](http://www.us-cert.gov/control_systems/cstraining.html).

---

## **Industrial Control Systems Articles**

ICSJWG is now accepting short articles of general interest pertaining to control systems security for the March quarterly newsletter. If you want to submit an article for the March newsletter, please email [icsjwg@dhs.gov](mailto:icsjwg@dhs.gov), and we will take your article into consideration for publishing. The deadline for submissions for the March newsletter is **February 25, 2010**.

Past ICSJWG newsletters are located on the CSSP website at [http://www.us-cert.gov/control\\_systems/icsjwg/index.html](http://www.us-cert.gov/control_systems/icsjwg/index.html) and on HSIN at <https://cs.hsin.gov/C10/C1/ICSJWG/default.aspx?RootFolder=%2fC10%2fC1%2fICSJWG%2fDocument%20Library%2fICSJWG%20Newsletters&View=%7b7F0225B9%2d1943%2d4074%2dB349%2d32C32A4EB8E7%7d>

The following articles were submitted by members of the ICSJWG for publication and distribution to the ICSJWG community. Thank you for contributing.

---

## **ISASecure Embedded Device Security Assurance (EDSA) Certification Program Is Operational**

*By Andre Ristaino, Managing Director, Automation Standards Compliance Institute*

During the October 2010 ICSJWG, the ISA Security Compliance Institute (ISCI) announced that the first industry based industrial automation control systems cyber security certification program was expected to be operational in Q4 2010. The program is operational and ISCI is currently assessing the first device submission from a global supplier of automation control systems with others slated for 2011.

The ISASecure program was developed by the ISA Security Compliance Institute (ISCI) with a goal to accelerate industry-wide improvement of cybersecurity for Industrial Automation and Control Systems (IACS). It achieves this goal by offering a common industry-recognized set of device and process requirements that drive device security, simplifying procurement for asset owners and device assurance for control systems suppliers.

The ISASecure Embedded Device Security Assurance Certification (ISASecure EDSA) is the first ISASecure certification in ISCI's certification roadmap. It focuses on security of embedded devices and assesses device characteristics and supplier development practices for those devices. The assessment consists of three elements; a device Functional Security Assessment (FSA), a device Communication Robustness Test (CRT) and, an organizational Software Development Security Assessment (SDSA) similar to ISO/IEC 61511.

Through this certification, an embedded device that meets the requirements of the ISASecure specifications receives the ISASecure EDSA certification—a trademarked designation that provides instant recognition of product security characteristics and capabilities. ISASecure EDSA offers three certification levels for a device based on increasing levels of device security assurance: ISASecure Level 1 for Devices, ISASecure Level 2 for Devices, and ISASecure Level 3 for Devices.

The ISASecure EDSA certification is an ISO/IEC Guide 65 conformance scheme supporting ISCI's goal to operate a globally recognized industrial automation controls cybersecurity certification program. This third-party accreditation by ANSI/ACLASS enhances the credibility and value of the ISASecure certification by attesting to the competence and qualification of ISCI certification bodies and laboratories. Visit <http://www.ansi.org/isasecure> or <http://www.isasecure.org/> for details on the ISASecure ANSI/ACLASS accreditation process.

Founded in 2007, the ISA Security Compliance Institute's mission is to provide the highest level of assurance possible for the cyber security of industrial automation control systems.

The Institute was established by thought leaders from major organizations in the industrial automation controls community seeking to improve the cyber security posture of Critical Infrastructure for generations to come. Founding Members include Chevron, ExxonMobil Research and Engineering, Honeywell, Invensys, Siemens, and Yokogawa. Key Technical Members include exida and Rockwell Automation.

The Institute's goals are realized through industry standards compliance programs, education, technical support, and improvements in suppliers' development processes and users' life cycle management practices. The Institute's ISASecure™ designation ensures that industrial automation control products conform to industry consensus cyber security standards, providing confidence to users of ISASecure™ products and systems and creating product differentiation for suppliers conforming to the ISASecure™ specification. <http://www.isasecure.org/>

---

# Cyber Security, Providing Value Through a Collaborative Team Approach

By Ernest A. Rakaczky, IOM Portfolio Program Manager, Invensys

Within the identified Critical Infrastructures of Nations around the world, control vendors with their control systems and application are continuously playing a vital role in their safe and reliable operations. Equally these same systems have come under the attention and realization that most could have a huge potential of a possible cyber security risk if strong cyber security measures are not put into practice.

**Homeland Security Presidential Directive 7 (HSPD-7) along with the National Infrastructure Protection Plan (NIPP) identified and categorized United States infrastructure into the following 18 critical infrastructure and key resources (CIKR) sectors...**

- |                                   |   |   |
|-----------------------------------|---|---|
| 1. <b>Agriculture &amp; Food</b>  | 7. <b>Emergency Services</b>                        | 13. <b>Postal &amp; Shipping</b>          |
| 2. <b>Banking &amp; Finance</b>   | 8. <b>Energy</b>                                    | 14. <b>Public Health &amp; Healthcare</b> |
| 3. <b>Chemical</b>                | 9. <b>Government Facilities</b>                     | 15. <b>Telecommunications</b>             |
| 4. <b>Commercial Facilities</b>   | 10. <b>Information Technology</b>                   | 16. <b>Transportation</b>                 |
| 5. <b>Dams</b>                    | 11. <b>National Monuments &amp; Icons</b>           | 17. <b>Water</b>                          |
| 6. <b>Defense Industrial Base</b> | 12. <b>Nuclear Reactors, Materials, &amp; Waste</b> | 18. <b>Critical Manufacturing*</b>        |



\* Critical Manufacturing was announced as the 18<sup>th</sup> Sector in April 2008

***“Many of the Processes Controlled by Computerized Control Systems Have Advanced to the Point that They Can No Longer Be Operated without the Control System”***

Taking a holistic approach to control system security is based on the following principles:

- View security from both management and technical perspectives
- Ensure security is addressed from both an IT and control system perspective
- Design and develop multiple layers of network, system and application security
- Ensure industry, regulatory and international standards are taken into account
- Prevention is critical in plant control systems, supported by detection
- Provide support and guidance in the establishment of Compliance with Industry requirements being established by – SP99, NERC CIP, NIST800, IAEA, DOE, etc...

In general view Cyber Security as a very strong on-going operational requirement embedded in the everyday operational procedures; like physical safety we see cyber security becoming an “Operational Way of Life”.

Until recently, many process control networks have been implemented with either no security or minimal security. One approach had been to keep the process control network separate from the

business network. While this has proven to be effective, current technology advances with open systems and the demand for information is driving tighter connectivity between the two networks. Devices in use on the process control network have the ability to gather real time information about the process and have the ability to adjust to commands to and from the business network.

Vendors need to establish the following steps to ensure their products and solutions are:

1. **Developed** – utilizing the best- in-class security development life-cycle program – SDL
2. **Tested** – through the National labs testing programs, Wurdtech device Certification & defined QA security specific testing
3. **Implemented** – using FAT & SAT security base-lining measures
4. **Supported** – required infrastructure in place to provide a lifetime of support
5. **Improved** – offering Modernization, Advantage & Migration programs

The key here is that these steps are being taken not in isolation but are being molded with a clear understanding and certainty of the current day requirements. This can be continuously validated by a very active participation, in working with the key groups in the overall definition, strategies, standards, etc... that is currently available today.

- DHS Department of Homeland Security
- DOE Department of Energy
- IAEA International Atomic Energy Agency
- NERC North American Electric Reliability Corporation
- ISA SP99 ISA Control System Security Standards
- ICSI ISA Security Compliance Institute
- NIST SMART GRID Security Working groups
- I3P Institute for Information Infrastructure Protection
- NPRA National Petrochemical & Refiners Association
- AF Automation Federation
- EWE WIB – EI – EXERA – Established Vendor Security Practice Program

### ***Being Involved:***

Over the past years there has been continuous progress being made in the establishment of governing practices, operational standards, procurement guidance's and industry awareness. This comes about from a very strong collaboration of efforts from within the user community, Governments, Standards bodies, Researchers, Academia and control system suppliers.

### ***Positioning Cyber Security Requirements as an Operational Value Addition:***

**When you're talking about cyber security in the process industries, there are really only two issues that matter. The first, rather obviously, is how much security you need to be really secure. The second issue isn't all that obvious, but in many ways defines the first...and it isn't one that people are really thinking about. What's the difference between "compliance" and "security"?**

To position the "compliance versus security question" correctly, one must first take compliance/compliancy and realize from the outset that there are multiple levels in being compliant, but that the number one focus always seems to be around that one snapshot in time-- the audit.

Holistically, compliancy is imperative for a successful cyber or physical security program. Being compliant can range from complying with an auditable set of federally mandated guidelines, like NERC/CIP, to simply complying with an internal policy or procedure that has been established within a security program. Compliancy requirements drive the overall management of a security program, and it is within these requirements that many necessary security measures will be established.

Here again people first look at security measures as a means to protect, and that is paramount, but security measures also need to include monitoring, correlation, rationalization, etc. That is how you can begin to evaluate if the investment in security outweighs the value of the assets you are trying to protect.

Compliancy can't guarantee that established security measures of an organization will never be breached. But compliancy and practical security measures serve as the foundation for a culture where everyone feels like they have an equal stake in the overall security and success of the operation. In a security culture, the security program is part of the plant's normal way of life.

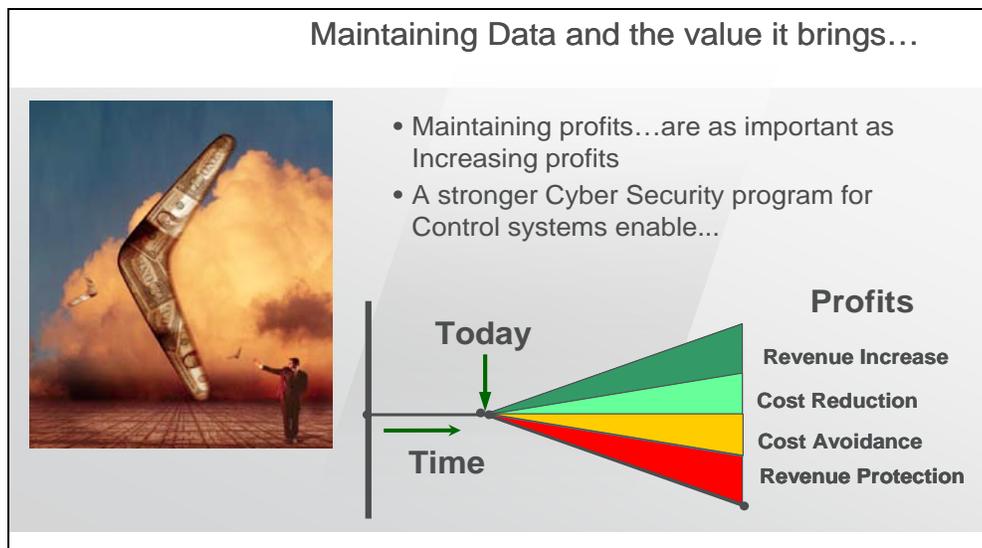
So how do you know if you have enough security to be really secure?

To answer that, we have to use the basic definition of Security as the degree of protection against danger, loss and criminals.

To understand, manage and reduce risk, the following elements need to be considered. It all comes down to:

- **Assurance** - the level of guarantee that a security system will behave as expected;
- **Countermeasure** - a way to stop a threat from triggering risk;
- **Defense-in-depth** - never relying on a single security measure, but on a layer of security measures;
- **Exploit** - a vulnerability that has been triggered by a threat;
- **Risk** - a possible event that could cause a loss;
- **Threat** - a method of triggering risk;
- **Vulnerability** - a weakness in a target that can potentially be exploited.

So how does this all play into determining security requirements?



For the most part, today's conversations on security focus on the cost of and/or burden of implementing security. Plant and enterprise managers know that something has to be done, but at the same time, they want to know what they can do to reduce the cost of their investment while still mitigating risk.

In some regards, just doing even a little will raise the security of the infrastructure substantially.



**Maintaining Data and the value it brings...**

- Enable process improvements to reduce process costs**
- Enable process improvements to increase production**
- Increased administration capacity by streamlining the security workload**
- Avoid current and increased costs of regulatory compliance and non-compliance**
- Protect production from the impact of increasing security intrusions**
- Protect the plant from a catastrophic event caused by a security intrusion**

Something that is frequently overlooked is the fact that today's control systems and their interconnectivity can be used not only to improve operations, i.e., controlling the process better to move more down the wire, out the pipe, etc, but also for improving the flow of business information across the enterprise. That means that data that has always been there is more valuable now, and when it all comes together from several plants, it allows an operation to make better, more fundamentally sound day-to-day business decisions. So what we really need to start doing is quantifying that data and the value it brings to an organization to help them make a solid business case for investing in security.

At its core, the basic security requirement is to protect the process and operation from disruptions and all the issues that derive from an event. Some of the risks within process controls are related to policies that require moving existing data out of the actual control systems, things like EPA reporting, historian information, production management information, etc.

It is safe to say that no plant is going to go back in time and reinstate operational procedures, as was common practice in the past, via manual logging, data transfer via manual recoding, trying to estimate a value on a pen chart, etc. The challenge today is to identify these common practices and clearly show how continual modernization has saved and enhanced the financial models of the operating organization. By doing that, we should start to see the clear value and importance of applying stronger security to reduce risk, maintain business continuity and provide the ability for greater visibility into process areas.

## **A New Cold War?**

*By Andrew Ginter, Chief Technology Officer, Abterra Technologies.*

*Some of this material was first published in Industrial Defender's "Findings From the Field" Blog.*

Many authors have described the sabotage-oriented Stuxnet worm as an example of "cyber warfare." It seems to me that if the 2009 Ghostnet and Aurora attacks and the 2010 Stuxnet attack represent a new "cyber warfare" then such warfare has more in common with the cold war era than with a conventional conflict. Thinking of the events of 2009-2010 as a cold war can help answer key questions like:

- When will we see new, sophisticated attacks?
- Who will be targeted?

### **The Stuxnet Worm:**

In version 1.3 of their W32.Stuxnet Dossier, Symantec reports that the Stuxnet worm targets PLCs which control high frequency, frequency-converting power supplies. Such high quality power supplies are export-controlled in the United States because they can be used as components in gas-centrifuge uranium enrichment processes. Symantec stops short of identifying Iran's uranium enrichment facilities as the target of the worm, but the information they supply is suggestive of such a target.

Symantec has decoded many of the function blocks the worm injects into Siemens Programmable Logic Controllers (PLCs). The rogue code seems to run the power supplies at less than the programmed frequency for a period of time, and then send out messages to change the frequency of the power supplies. The logic sometimes runs the power supplies at a higher frequency than their setpoints, and sometimes issues commands to very suddenly slow them down and then speed up them up again.

Open source literature suggests that if the manipulated power supplies are indeed powering centrifuges, then there are three consequences we can expect from such manipulations. Running the centrifuges too slow defeats their purpose and results in no enrichment of the uranium. Running them even 20% faster than their setpoint can tear the centrifuges apart. Finally, changing the power supply frequency suddenly to very low and then very high values can induce vibrations sufficient to destroy the centrifuges as well.

There is very little evidence as to who were the authors of the worm. Symantec has described the worm as the most sophisticated piece of malware they have ever encountered. They estimate that a team of 6-10 primary developers took at least six months to develop the worm. There is no estimate as to how many secondary QA and other developers were involved. My own experience with developing sophisticated software that must run "clean" on platforms from Windows 2000 all the way through Windows 7 is that the QA effort was at least twice that of the original software development. The size and sophistication of the team, and the assumed target suggests a western government's military or intelligence agency authored the worm.

## ***A New Cold War:***

I regard the most sophisticated attacks of 2009-2010 as a cold war because of type of attack and because of the agencies presumed to be responsible.

- The Ghostnet attack targeted embassies and foreign ministries of a number of governments, and was widely, but not conclusively, attributed to the Chinese government.
- The Aurora attack targeted large technology firms, apparently stealing source code and other intellectual property, and was widely, but not conclusively, attributed to the Chinese government.
- The Stuxnet attack appears to have targeted Iranian uranium enrichment facilities, and is thought to have originated with a western government, most likely the USA or Israel.

In all cases governments are thought to be responsible. Criminal organizations continue to account for a continuous stream of new malware of steadily increasing sophistication. However, the step changes in sophistication we have observed in the last two years have all been attributed to governments, not criminals. In all three cases the attacks were specifically targeted. The apparent motive was in two cases information theft or “intelligence gathering,” and in the third, damage to a militarily-sensitive installation.

All of these tactics and motives are more reminiscent of cold war tactics than of some full-scale modern warfare. The cold war was characterized by only indirect conventional conflicts between the three cold war powers, by continuous and aggressive intelligence-gathering, and by occasional sabotage of military and civilian infrastructure. In trying to understand whether new, very sophisticated attacks will be seen in the next year or two, bear in mind:

- Many governments have announced they are developing “cyber warfare” capability, and many others are suspected of developing such capabilities unannounced,
- All of the three most sophisticated attacks of the last two years are presumed to have succeeded at least partially, and
- None of the authors of those attacks appear to have suffered significant consequences as a result of launching the attacks.

This suggests that in the years ahead we will see more of these kinds of attacks, from a greater variety of actors.

## ***Industrial Control Systems:***

I do not think we will see any credible attacks arise out of a manipulation of the Stuxnet worm itself. There are reports of researchers and others experimenting with the Stuxnet worm, substituting different parts of the payload and re-packaging the worm. However, any such “bragging rights” experiments, even if one is released into the wild, will have limited impact. Patches are available for four of the five Microsoft vulnerabilities the worm exploited. That means a repackaged worm will have a very hard time propagating on enterprise networks any more, and such propagation is assumed to be essential to eventually compromising the targeted control network.

What is not clear is whether civilian industrial sites will be targeted by cyber-cold-war powers. In the last cold war, civilian infrastructure was generally targeted only in those geographies involved in active conventional conflict. The exception to this rule is the still-unconfirmed case of the Siberian

natural gas pipeline explosion, said to be triggered by a CIA-planted trojan in the SCADA software.

That said, in today's western democracies and in the USA in particular, nuclear sites and military sites tend to be much better protected than important civilian control systems. When cyber-cold-war powers look for western targets, will they confine their activities to military targets? Or they will see civilian industrial control systems as much easier prey and so target them?

### ***Defending Against Sophisticated Attacks:***

To defend civilian control systems from sophisticated attacks like the Stuxnet worm takes a much stronger defense-in-depth posture than is the current, regulated best practice. The most urgently-needed improvements in best practices are greater use of whitelisting/HIPS technologies, greater network segmentation and stronger programs controlling the use of removable media.

All defenses have costs to implement, but it seems to me that the “greater network segmentation” defense may face the greatest resistance. Truly secure sites, like most nuclear and military sites, have serious restrictions as to what kind of information can be exchanged across security perimeters. In contrast, enterprise integration and the widespread commercial exploitation of valuable control system data has been taken for granted for years now at most industrial sites. Reducing the amount and kind of information that flows between security zones in civilian control systems will be difficult and costly.

It seems clear that a new kind of international conflict is developing. Even if we suspect that civilian control systems will not be targeted for the next year or two, it would be prudent for civilian sites take advantage of this time. Civilian sites which represent the greatest threat to public safety should use the next year or two to invest in protections sufficient to ward off sophisticated attacks by foreign governments

---

### ***Participation is Key!***

Your participation and input is **critical** to the success of these subgroups and to the overall mission of ICSJWG to coordinate cyber security efforts to secure ICS across the nation's critical infrastructure. Please email the co-chairs or [icsjwg@dhs.gov](mailto:icsjwg@dhs.gov) to get involved with one or more of the subgroups.

---

### ***CSSP Contact Information***

If you would like to contact the ICSJWG to ask a question or inquire about participation, please send an e-mail to [icsjwg@dhs.gov](mailto:icsjwg@dhs.gov).

The CSSP and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) encourage you to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems. Online reporting forms are available at <https://forms.us-cert.gov/report/>.

Other important contact information:

Web Site Address: [http://www.us-cert.gov/control\\_systems/](http://www.us-cert.gov/control_systems/)

ICS-CERT Email: [ics-cert@dhs.gov](mailto:ics-cert@dhs.gov)

Phone: 1-877-776-7585

CSSP Email: [cssp@dhs.gov](mailto:cssp@dhs.gov)

*Thank you for your participation and making this a  
great year.*

*Happy Holidays from ICSJWG!*

