Strengthening Cyber Incident Response Capabilities Through Education and Training in the Incident Command System

Austen D. Givens

Supervisory Control and Data Acquisition (SCADA) systems control innumerable industrial processes that affect large segments of U.S. critical infrastructure, from regulating the flow of water through dams to calibrating the electrical currents in power substations located in residential neighborhoods. Historical evidence demonstrates that electronic attacks on SCADA systems can physically damage them. This can trigger consequences that must be simultaneously addressed by Computer Security Incident Response Teams (CSIRTs) and traditional first responders. This article advances a two-part argument: first, that the Incident Command System (ICS) offers a compelling means to strengthen cyber incident responses by integrating CSIRTs and first responders involved in SCADA incidents into a cohesive organizational structure; and second, that cybersecurity curricula in academic and professional training settings should therefore incorporate ICS education in order to increase the probability of effective incident responses involving CSIRTs and first responders in the future.

Introduction

An oil pipeline running through central Siberia exploded one night in October 1982, sending an enormous fireball into the sky (National Security Archive, 2013). The blast was so powerful that it released the energy equivalent to that of a small atomic bomb (National Security Archive, 2013). The Central Intelligence Agency (CIA), in what may be the world's first-ever example of cyber sabotage, made the pipeline explode by introducing flawed computer code into the pipeline's control system, causing its components to malfunction (National Security Archive, 2013). This attack took advantage of electronic vulnerabilities in the pipeline's Supervisory Control and Data Acquisition (SCADA) systems, which regulated the movement of turbines in the pipeline that kept oil flowing from one point to another (National Security Archive, 2013). The CIA was able to exploit these vulnerabilities with the flawed computer code, causing the SCADA system to malfunction, ultimately resulting in the pipeline explosion.

Twenty eight years after the Siberian pipeline explosion, the U.S. government again used flawed computer code to damage physical infrastructure—this time, in Iran. In June 2010 Iranian nuclear officials discovered that many of the centrifuges that they were using to purify uranium had been badly damaged (Fildes, 2010). The U.S. and Israeli governments, which believed that Iran was using the uranium to build nuclear weapons, co-wrote and introduced a virus called Stuxnet into the centrifuge control systems (Fildes, 2010; Ferran & Radia, 2013). This highly sophisticated computer virus caused the centrifuges deliberately to spin out of control, breaking them (Fildes, 2010). The damage

was so widespread that one expert speculated that Stuxnet set back the progress of the Iranian nuclear program by two years (Katz, 2010). The Iranian government, however, denied that the damage had any serious impact on its nuclear ambitions (Warrick, 2011). Outside analysis by the Royal United Services Institute, a London-based defense think tank, confirms that Stuxnet's true long-term impact on the Iranian nuclear program was negligible (Barzashka,

The Siberian pipeline explosion and the Stuxnet virus demonstrate that attacks on SCADA systems can be used to cause physical damage to infrastructure. The risk of this type of damage is of increasing concern to U.S. federal officials. The Department of Homeland Security (DHS) recently ran a worldwide exercise to test response coordination to just such an incident (DHS, 2014). The need to prepare for physical infrastructure damage caused by SCADA system attacks gives rise to a fundamental question about cyber incident response capabilities in the United States: how are computer security experts, tasked with responding to the virtual effects of cyber attacks, and traditional first responders, who attend to the physical consequences of these incidents, to integrate their actions effectively?

This article argues that the Incident Command System (ICS), which has for years been used to manage conventional disasters, provides a ready-made and effective organizational structure for computer security experts and traditional first responders to integrate their responses to SCADA system attacks. Moreover, this article makes the case that since ICS can be used to blend the response actions of computer security experts and first responders, ICS training should be an integral part of cybersecurity curricula, precisely because of the rising need for computer experts and first responders to work closely with one another.

The rest of the article proceeds as follows. Part two briefly introduces ICS and frames the contribution of this study within the literature on ICS. Part three shows how ICS can effectively integrate cybersecurity experts and first responders into a single incident response framework. Part four makes the case that educational institutions and professional certification organizations should make ICS a central component of their cybersecurity curricula. The article concludes by synthesizing the key themes presented in this analysis and offers recommendations for future research in this area.

ICS is a method, or way, to respond to emergencies. It superimposes an organizational coordinating structure on the uncertain and ever-changing conditions of an incident. Superimposing this management structure on the incident response permits one or more organizations to work together in a more streamlined, effective fashion. Moreover, ICS has been used successfully for at least 30 years, demonstrating that it is a viable way to manage emergency responses of any size or scope.

After the 9/11 terrorist attacks, ICS became a central focus of federal efforts to streamline and enhance incident response coordination. This renewed focus on ICS was in part a direct reaction to many of the coordination failures observed on 9/11, such as poor communication and collaboration among local government agencies in Manhattan following the collapse of the World Trade Center Twin Towers (9/11 Commission, 2004, pp. 319–322). Calls for a national standard in incident management led to the development of the National Incident Management System (NIMS) in 2004 (DHS, 2003; 9/11 Commission, 2004,

Today NIMS is a national approach to incident management that covers all jurisdictions and functional areas (DHS, 2008). ICS is a central focus of NIMS (DHS, 2008b, pp. 45–63). In recent, notable large-scale incidents in the United States, public safety officials used ICS in response to Hurricane Katrina in 2005 and the powerful Joplin, Missouri tornado of 2011 (9/11 Commission, 2004; C-SPAN, 2011; DeAtley, 2011, pp. 12–13). Government agencies also use ICS throughout the United States on more routine, everyday emergencies, from house fires to hostage standoffs. And most recently, in the 2010 draft National Cyber Incident Response Plan (NCIRP), the U.S. Department of Homeland Security (DHS) identifies ICS as the response methodology of choice for managing significant cyber incidents (DHS, 2010, p. 16).

Figure 1 below depicts a prototypical ICS organizational structure. While detailed explanations of the specific positions shown in this ICS structure are beyond the scope of this article, what is noteworthy—and applicable directly to the management of SCADA incidents—is that ICS incorporates a diversity of actors performing distinct and complementary functions in the context of an incident response effort.

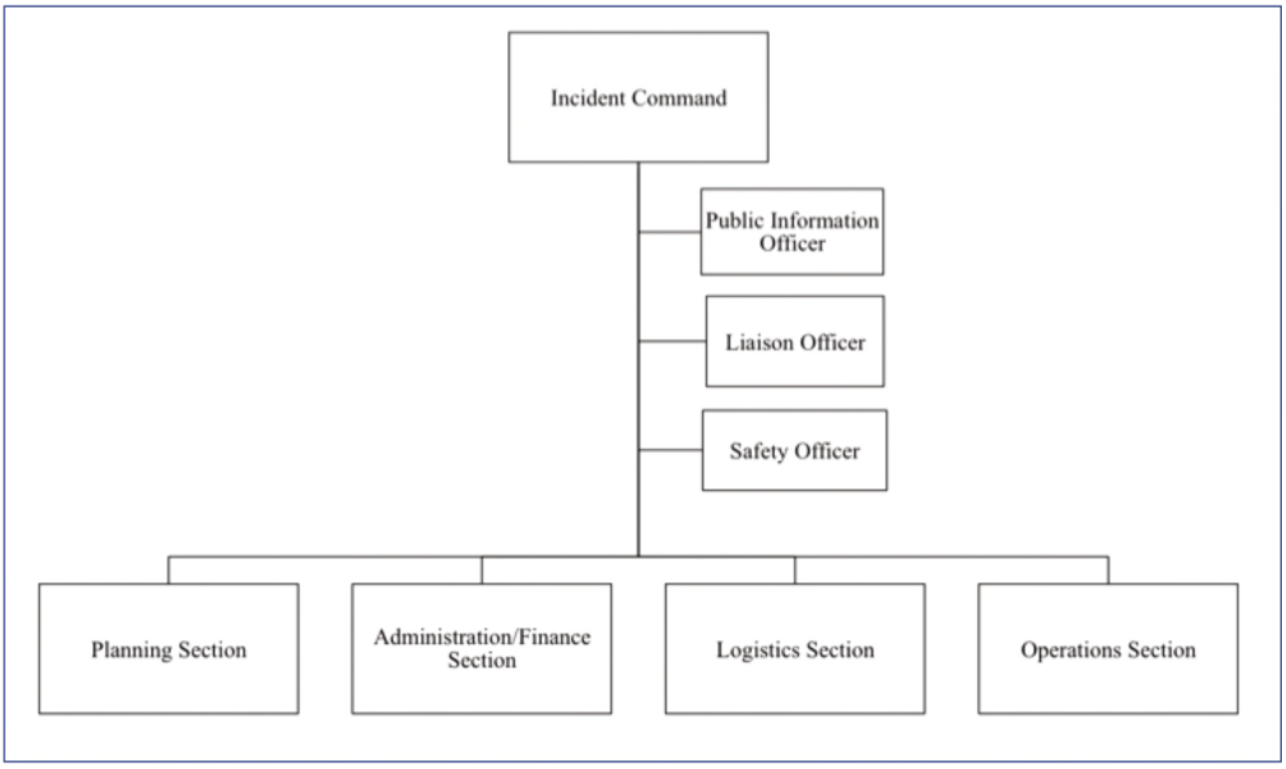
The Siberian pipeline explosion and Stuxnet examples introduced at the beginning of this article demonstrate that cyber incidents can have real-world consequences for the operation of critical infrastructure, particularly in the realm of SCADA systems. SCADA incidents can therefore require a coordinated response effort among computer security incident response teams (CSIRTs), which are specialized groups of information technology (IT) professionals that manage cyber incidents, and traditional first responders, like police officers, firefighters, and EMTs. This confluence of factors suggests that ICS may be a viable method to coordinate the actions of CSIRTs and first responders. Contemporary research on ICS, as well as government reports on cyber incident management, underscores that new understandings of how ICS may be used in response to SCADA incidents are needed.

CONTEMPORARY SCHOLARSHIP ON THE INCIDENT COMMAND SYSTEM

Research on ICS tends to emphasize one of three primary themes. First, ICS must be adapted to the unique local circumstances in which it is being used, taking into consideration factors such as the scope of the emergency and the jurisdictions involved in the response. Second, despite the strengths of ICS, the system also suffers from a number of serious deficiencies that may limit its effectiveness under certain conditions. And third, analyses of ICS's organizational structure show that the system combines elements of vertical organizational hierarchies and horizontal organizational networks, which may prove especially advantageous in responding to SCADA incidents.

Many authors address the customization of ICS to the needs of specific government agencies (Lam et al., 2010; Bauer, 2009; Esposito, 2011; Yates 1999; Ullman, 1998). Other scholars, however, critique ICS for its lack of customizability. For example, at least one author notes that ICS may be unsuitable for response to cyber incidents (Coleman, 2010). Still others take issue with ICS' inability to address

FIGURE 1: PROTOTYPICAL INCIDENT COMMAND SYSTEM (ICS) STRUCTURE



higher-level command structures beyond that of the incident itself; the very notion that an incident can be controlled within any type of framework; the natural limits of ICS to adapt quickly to especially demanding incidents, such as nuclear, chemical, or biological attacks; ICS' inability to absorb volunteers; its utility being applicable only to para-military types of organizations; and the need for extensive organizational training in order to realize its benefits (e.g. Lutz & Lindell, 2008; Cole, 2000; Favero 1999; Yates, 1999).

A recent notable disaster—the 2010 Deepwater Horizon oil rig explosion and spill—highlights the complex forces influencing field use of ICS and underlines the salience of these observations (Givens, 2011; Baron, 2010). Descriptions of how ICS blends both elements of hierarchies and networks are useful, too, because they can enhance understandings of how ICS can be leveraged for SCADA incident responses (Moynihan, 2007, 2008, 2009, 2009b).

Government reports on recent exercises to evaluate cyber incident responses say nothing about ICS's suitability for emergencies concurrently affecting SCADA systems and the physical world. Indeed, three full-scale exercise reports from DHS spanning 2006–2011 do not specifically mention ICS at all (DHS, 2011; DHS, 2009; DHS, 2006). These documents do, however, underscore the continuing need for improved communication, coordination, and information sharing in response to incidents affecting critical infrastructure in the physical world and cyberspace. In particular, they highlight the unique challenge of maintaining a baseline of situational awareness across all response entities during a large-scale emergency (DHS, 2011; DHS, 2009; DHS, 2006). While greater knowledge of ICS's field-based utility and adaptability is helpful, existing literature fails to explain how CSIRTs and first responders might effectively integrate their actions within an ICS structure during a SCADA incident.

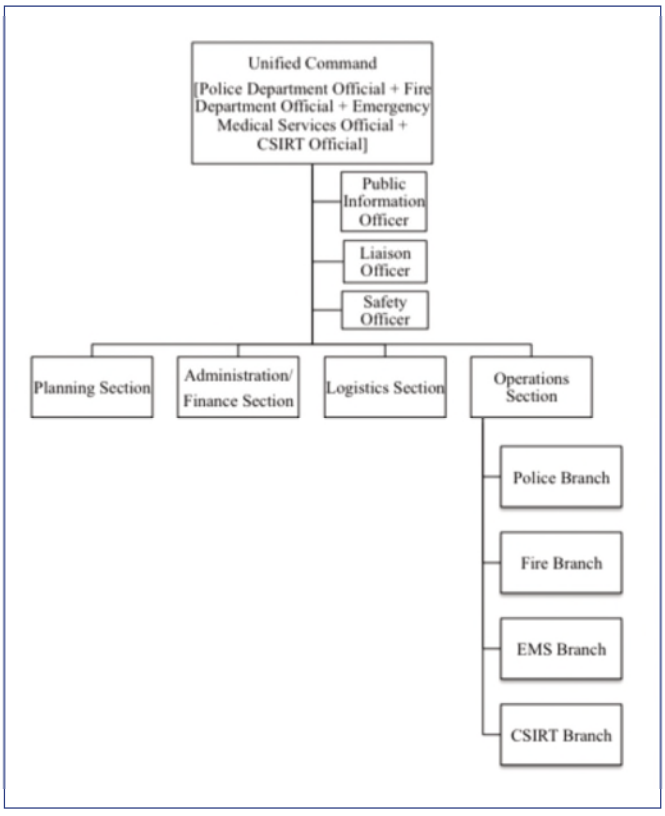
Unfortunately, there do not appear to be any published case studies of how ICS has been used to integrate the actions of one or more CSIRTs and traditional first responders managing a SCADA incident. This is understandable, however, because the idea of CSIRTs and traditional first responders coordinating a shared response to a SCADA incident is still relatively new. But to illustrate how this coordination between a CSIRT and first responders could work, let us next consider a hypothetical example.

INTEGRATING CSIRTS AND FIRST RESPONDERS USING THE INCIDENT COMMAND SYSTEM

ICS can be modified easily to integrate CSIRTs and first responders into a unified command structure. Figure 2 adjusts the prototypical ICS structure and shows how this integration occurs. For example, let us assume that a computer hacker maliciously attacks a SCADA system regulating the flow of water out of a dam. This electronic attack, in turn, causes the dam to release a torrent of water into a downstream community, causing flooding. Under this scenario, a linkage exists between this cyber attack and its physical effects. A CSIRT will need to manage the cyber attack on the SCADA system and traditional first responders will need to address flooding in this downstream community.

FIGURE 2:

INCIDENT COMMAND SYSTEM (ICS) STRUCTURE—INTEGRATING A COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT) AND TRADITIONAL FIRST RESPONDERS



The CSIRT integrates into the ICS structure as a branch within the Operations section, visible in the bottom right corner of Figure 2. Additionally, a CSIRT member joins other members of the Unified Command, visible in the top center of Figure 2. CSIRT members in the Operations section work on the cyber component of this incident by managing the hacker's attack on the SCADA system. They work to halt the hacker's progress and to restore the flow of water out of the dam to normal, pre-incident levels. Striving to mitigate a future, similar attack, they examine software code in concert with a vendor to ensure security patches are properly installed. After the incident has ended and recovery has begun, they conduct a formal after-action analysis to confirm that network vulnerabilities have been adequately closed.

While the CSIRT members address the cyber component of this incident, first responders contend with the physical effects of the cyber attack. Police officers re-direct traffic. Firefighters assist with swift water rescue of citizens trapped in their homes. Emergency medical personnel attend to the injured. Each of these distinct responses—the actions taken by the CSIRT, and the actions taken by first responders—forms part of a larger, integrated ICS structure.

ICS is useful for this kind of incident because of its scalability. Responses to SCADA system attacks incidents can involve fuzzy lines of jurisdiction and control, complicating response efforts (DHS, pp. 6–7). Thus a computer server owned by Firm A, manufactured by Firm B, cooled by equipment from Firm C, connected to a computer network via hardware from Firm D, and serviced by contractors from Firms E and F, can control a dam under the jurisdiction of Town G, which is located upstream from Villages H, I, and J. When this server's failure triggers effects in the physical world, it is challenging to organize and coordinate response agencies and organizations. Yet when necessary, ICS rapidly scales geographically, and it can efficiently incorporate these different actors into a unified response effort.

ICS is also helpful in this hypothetical incident because it can successfully integrate the actions of teams performing very different functions. CSIRT team members and traditional first responders like police officers, firefighters, and emergency medical personnel have divergent professional responsibilities. Since ICS can incorporate diverse groups of responders, including CSIRT team members and traditional first responders, it can be used to bring the efforts of these different functional groups together within a focused response coordination structure.

ICS offers a viable way forward for CSIRTs and first responders to synchronize their response efforts during a SCADA system attack. ICS can easily expand to group CSIRTs and first responders into a unified organizational structure. The system is able to accommodate teams of professionals from numerous organizations and jurisdictions, even when they are spread across a wide geographical area. And ICS permits professionals performing radically different jobs to work together toward common objectives. On its face, ICS appears to offer an effective method for CSIRTs and first responders to collaborate during SCADA system incidents.

Having made the case that ICS offers a potential solution for CSIRTs and first responders to integrate better their responses to SCADA system incidents, the next section argues that ICS training should be an essential component of professional education for cybersecurity professionals.

While numerous cybersecurity professional certifications exist, none appear to offer training in ICS. This is puzzling, since DHS has signaled clearly that ICS is the preferred response method for cyber incidents of any size or scope. Moreover, even certifications for those personnel specifically handling cyber incident responses do not appear to include ICS as part of their curricula. Table 1 lists four of the most popular IT security certifications and shows that these certifications do not include training in ICS.

TABLE 1:

CERTIFYING BODY	CERTIFICATION	RELEVANT BASIC TRAINING REQUIREMENTS	EVIDENCE OF ICS TRAINING? (YES/NO)	INFORMATION SOURCE(S)
Institute	GIAC Certified Incident Handler	Incident Handling Overview, Identification, and Containment		SANS Institute, 2014
	Certified Information Systems Security Professional (CISSP)	Domain experience in 2 of 10 functional areas, including business continuity/ disaster recovery		, 2014b
	Security +	Access control, identity management, cryptography, mitigation/deterrent techniques		
EC-Council	Certified Incident Handler	Incident Response, Incident Handling, Incident Categories		EC-Council, ND

The GIAC Certified Incident Handler credential is prestigious, in that it comes from the SANS Institute, one of the most widely recognized and peer-respected cybersecurity organizations (Symantec, 2012). The qualifications for this certification require cybersecurity professionals to show knowledge and proficiency in multiple functional areas, including the "steps of the incident handling process" and "common attack techniques that compromise hosts" (SANS Institute, 2014). These types of functional knowledge are to be expected, since they are indispensable for successful cyber incident management. However, the SANS Institute website detailing the requirements for this credential do not identify knowledge of ICS as a key requirement for the certification.

The CISSP is arguably the most recognizable credential among cybersecurity professionals (Nemeth et al., 2010, p. 945). The process to earn the CISSP is long and rigorous. In addition to passing an exam, prospective CISSP candidates must obtain at least five years of direct, full-time work experience in 2 of 10 knowledge domains (ISC , 2014b). These knowledge domains are: access control; telecommunications and network security; information security governance and risk management; software development security; cryptography; security architecture and design; operations security; business continuity and disaster recovery planning; legal, regulations, investigations, and compliance; and physical (environmental) security , 2014b). Of these 10 knowledge domains, the business continuity and disaster recovery domain is most directly applicable to ICS since ICS itself was born out of the need to respond more effectively to traditional disasters, such as fires and earthquakes. Nevertheless, the ISC website does not mention training in ICS at all.

CompTIA's Security + credential is not viewed universally to be among the strongest security credentials for IT professionals (Anderson, 2010). The credential is still popular, however, due in part to its reasonable cost (Anderson, 2010). The Security + certification covers several fundamental areas of cybersecurity, including access control, identity management, cryptography, incident mitigation, and deterrent techniques (CompTIA, 2014). However, there is no indication on the CompTIA website that ICS training is part of the Security + curriculum. CompTIA also does not appear to offer other certifications that would be more relevant or useful for cyber incident management purposes.

EC-Council's Certified Incident Handler credential uses a classroom and lab-based learning model over a two-day period (EC-Council, 2014). The organization's website includes a detailed agenda for the two day training period, and this agenda lists a significant

amount of instruction about how to form CSIRTs, incident response methods, and how to identify and categorize incidents that occur (EC-Council, n.d., pp. 3–6). But nowhere in this detailed training agenda does EC-Council mention ICS, its applicability to cyber incidents, or the ways in which ICS can integrate the efforts of CSIRTs and traditional first responders.

Four of the top cybersecurity professional certifications do not appear to identify or address explicitly the need for cybersecurity professionals to be proficient in ICS. One might expect colleges and universities, which recently have seen a great surge in growth of cybersecurity degree programs, to fill this gap in knowledge by including ICS instruction in their undergraduate and graduate-level curricula. It appears, however, that at least among the top five cybersecurity degree programs in the country, none have incorporated ICS training into their course syllabi.

A 2014 study by the Ponemon Institute, an independent Michigan-based research center focusing on IT security issues, ranked the top collegiate cybersecurity programs in the nation (Ponemon Institute, 2014). The data to construct the rankings came from a survey of IT security practitioners (Ponemon Institute, 2014, pp. 1–2). The top five schools in the rankings, in descending order, were: the University of Texas at San Antonio, Norwich University, Mississippi State University, Syracuse University, and Carnegie Mellon University (Ponemon Institute, 2014, p. 1). A web-based survey of these institutions' cybersecurity curricula suggests that ICS training is not being included in higher education curricula for cybersecurity. Table 2 lists the top five schools in the Ponemon Institute rankings, identifies classes within their curricula that relate to incident responses, and identifies those institutions that explicitly include ICS as part of their coursework.

TABLE 2:

INSTITUTION	RELEVANT DEGREE PROGRAM(S) OFFERED	COURSE(S) RELATED TO CYBER INCIDENT MANAGEMENT	EVIDENCE OF ICS TRAINING BEING OFFERED? (YES/NO)	SOURCE(S)
	BBA Cybersecurity, MS Information Assurance, BS and MS in Computer Science with security concentration	Principles of Computer Information Security, Introduction to Digital Forensics, Intrusion Detection and Incident Response		UTSA, n.d.; UTSA, n.d.-b; UTSA, n.d.-c; UTSA, n.d.-d; UTSA, n.d.-e
	Computer Security and Information Assurance undergraduate major and minor	Information Assurance I and II		Norwich University Norwich University 2014b
	BS Computer Science, BS Software Engineering, MS Computer Science	Business Information Systems Security Management		MSU, 2014b;
	MS Cybersecurity, Certificate of Advanced Study in Information Security Management	Computer Security, Internet Security		SU, 2015b
	MS Information Security	Network Forensics, Cyber Forensics and Incident Response Capstone		CMU, 2014b

The University of Texas at San Antonio houses the top-ranked cybersecurity degree programs in the United States (Ponemon Institute, 2014, p.1). These programs include a Bachelor of Business Administration degree in Cybersecurity, as well as a Master of Science degree in Information Assurance (UTSA, n.d.-b; UTSA, n.d.-c). UT San Antonio features several courses that pertain to cyber incident management, as well. These courses include Introduction to Digital Forensics, which teaches students how to analyze systematically the aftermath of a cyber incident, as well as Intrusion Detection and Incident Response, which deals precisely with the topic of responding to cyber incidents (UTSA, n.d.-e). Among the descriptions of these degree programs and courses, however, there is no mention of ICS. Norwich University, Mississippi State University, Syracuse University, and Carnegie Mellon University round out the top five cybersecurity academic programs in the United States. None of these institutions appears to offer any instruction in ICS for cybersecurity students, either.

There are several possible explanations for the absence of ICS instruction in these top cybersecurity degree programs. The simplest and most plausible explanation is that these institutions *do* train students in ICS within their courses, but they do not make that fact publically known on their websites. It is also possible that universities are reacting to changing marketplace demands in cybersecurity, and this reacting creates a lag effect between the emergence of a market-driven need for training in ICS and universities ultimately incorporating ICS training into their curricula. This explanation seems less probable, though. The NCIRP, which specifically identified ICS as the response method of choice, was published in 2010—four years before this writing, and a reasonable amount of time for universities to adopt and incorporate ICS training into their courses. A third possible explanation is that training in ICS is seen as too "practitioner-driven" for a university setting and somehow lacking in academic rigor or legitimacy. Yet this explanation rings hollow, as Norwich University and Syracuse University are known for being "military-friendly" institutions with many students that come from practitioner-oriented backgrounds in the U.S. armed services (Jevis, 2014; Norwich, 2014).

It is clear that the top cybersecurity professional certifications and cybersecurity academic programs in the United States either do not include ICS training as part of their course curricula; or, at a minimum, these certifications and degree programs do not place great emphasis on the fact that this ICS training is included in their courses. Given the need for CSIRTs and first responders to synchronize their responses to SCADA incidents, this gap in ICS training should be corrected by the certifying bodies and universities themselves. To support these certifying bodies and universities in their efforts, however, DHS and the Department of Defense (DOD) can offer three forms of low- or no-cost assistance.

DHS and DOD can help to push knowledge of ICS to cybersecurity certification groups and universities through incentives, web-based resources, and hands-on training. If it costs certification organizations money to make changes to their curricula, then they must have a compelling reason to make these modifications. DHS and DOD can offer one-time cash awards, in the form of grants or prizes, to groups like and institutions of higher education to make these changes quickly. This "free money" would go a long way toward overcoming organizational inertia to making curricular modifications, and would not act as a long-term financial burden on the federal government, because the awards themselves would be one-time-only cash allocations. DHS and DOD can also make available web-based resources for ICS training. DHS already makes available online ICS resources for first responders and others in the emergency management community (DHS, ND). Tailoring this information slightly to a cybersecurity-oriented audience could be helpful in encouraging CSIRTs to adopt ICS. Lastly, DHS and DOD could offer occasional hands-on training in ICS for CSIRTs. To encourage attendance, these agencies would have to offer the training so that it is convenient for CSIRTs to attend, and at little or no cost. DHS already conducts these hands-on ICS trainings, often through state-level emergency management agencies, for first responders and emergency managers (VDEM, 2012). Adapting the existing hands-on ICS training for CSIRTs could also go a significant way toward encouraging CSIRTs to adopt ICS.

This article argued that CSIRTs should use ICS during SCADA incidents, because doing so makes it easier to integrate CSIRT actions with those of traditional first responders. Although this arrangement may present select communication and coordination challenges for CSIRTs and first responders, on balance ICS will help CSIRTs and first responders to manage SCADA incidents more effectively. To facilitate the use of ICS by CSIRTs, the nation's top professional cybersecurity certification groups and universities offering cybersecurity degrees should make ICS an explicit part of their curricula.

There is a compelling need for additional research in this area, because little is known about the process by which the field-based findings of homeland security and cybersecurity practitioners eventually integrate into educational and training programs. In particular, the absence of case studies about how lessons learned from specific incident responses feed into educational programs in homeland security and cybersecurity is problematic. Scholars and practitioners can benefit from deeper investigations of how these lessons learned in real world incidents can be integrated better into formal educational settings.

The cybersecurity and emergency management communities can also benefit from greater knowledge exchange. It has been said that ICS can be a way of thinking about incident management, as well as a way of coordinating response to an incident. In other words, ICS is not merely a management tool for dealing with an incident; ICS also conveys a cultural approach to incident management that emphasizes principles like flexibility, adaptability, and creativity. How can CSIRTs learn to "do" ICS, and also embrace these principles in their own cultural approach to incident management?

One possible first step is for CSIRT members in government agencies and the private sector to take independent study courses online through the Federal Emergency Management Agency's (FEMA) Emergency Management Institute as part of their normal training activities. These emergency management courses, which are available for free, can provide CSIRT members with introductory knowledge of the principles found in NIMS, the NRF, and ICS (FEMA, 2012). In completing these courses, CSIRT members can develop more sophisticated and nuanced understandings of how ICS can be beneficial for them. CSIRT members can also gain helpful insights into how first responders use ICS during incidents. Important principles of emergency management like flexibility and resiliency can become more inculcated in a CSIRT's culture as a result of this training. And this training, in turn, can help CSIRTs to better integrate their operations with traditional first responders, and to achieve better results in managing incidents.

As SCADA incidents become increasingly common, there will be a pressing need for CSIRTs and traditional first responders to coordinate their response actions. ICS, a proven method for managing incidents of any size, scope, or cause, can help CSIRTs and first responders to better integrate their efforts and strengthen homeland security as a result. It is now essential that cybersecurity training and education programs embrace ICS to prepare their students for joint responses with homeland security practitioners.

Anderson, N. (2010, January 26). Thought that A+ cert was good for life? Think again. *Ars Technica*. Retrieved from http://arstechnica.com/tech-policy/2010/01/thought-that-a-cert-was-good-for-life-think-again/

Bauer, T.P. (2009). *Is NIMS going to get us where we need to be?: A law enforcement perspective* (master's thesis). Naval Postgraduate School, retrieved from the Homeland Security Digital Library.

Baron, G. 2010. (2010, May 14). Deepwater and the future of NIMS. *Emergency Management*. Retrieved from http://www.emergencymgmt.com/emergency-blogs/crisis-comm/Deepwater-and-the-Future.html

Barzashka, I. (2013). Are cyber weapons effective? Assessing Stuxnet's impact on the Iranian enrichment program. *The RUSI Journal*

Carnegie Mellon University. (2014). CyLab. Retrieved from https://www.cylab.cmu.edu/education/index.html

Carnegie Mellon University. (2014b). MSIS Core Course Descriptions. Retrieved from http://www.ini.cmu.edu/degrees/msis/courses.html#forensics

Cole, D. (2000). *The Incident command system: A 25 year evaluation by California practitioners*. Retrieved from http://www.usfa.fema.gov/pdf/efop/efo31023.pdf

Coleman, K. (2010, October 18). Cyber incident responders lack a shared playbook. *DefenseSystems*. [Commentary]. Retrieved from http://defensesystems.com/articles/2010/10/15/digital-conflict-cyber-incident-response.aspx

CompTIA. (2014). CompTIA Security +. Retrieved from http://certification.comptia.org/getCertified/certifications/security.aspx

C-SPAN. (2011, March 16). Louisiana Incident Command Post. Retrieved from http://youtu.be/_ctvFT_Sq7w

DeAtley, C. (2011). 45 seconds of danger, a lifetime of lessons. *DomPrep Journal*

Department of Homeland Security. (2014). *Cyber storm: Securing cyber space*. Retrieved from http://www.dhs.gov/cyber-storm-securing-cyber-space

Department of Homeland Security. (2011). *Cyber storm III: Final report*. Retrieved from http://www.dhs.gov/sites/default/files/publications/CyberStorm%20III%20FINAL%20Report.pdf

Department of Homeland Security. (2010). *National cyber incident response plan [Interim Version]*. Retrieved from http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf

Department of Homeland Security. (2009). *Cyber storm II: Final report*. Retrieved from http://www.dhs.gov/sites/default/files/publications/Cyber%20Storm%20II%20Final%20Report.pdf

Department of Homeland Security. (2008). *National incident management system* [Brochure]. Retrieved from http://www.fema.gov/pdf/emergency/nims/NIMS_brochure.pdf

Department of Homeland Security. (2008b). *National incident management system*. Retrieved from https://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf

Department of Homeland Security. (2006). *Cyber storm exercise report* Retrieved from http://www.dhs.gov/sites/default/files/publications/Cyber%20Storm%20I%20After%20Action%20Final%20Report.pdf

Department of Homeland Security. (2003, February 28). *Homeland Security Presidential Directive 5: Management of Domestic Incidents* Retrieved from http://www.dhs.gov/sites/default/files/publications/Homeland%20Security%20Presidential%20Directive%205.pdf

Department of Homeland Security. (n.d.). *ICS resource center.* Retrieved from http://training.fema.gov/EMIWeb/is/ICSResource/

EC-Council. (2014). *EC-Council certified incident handler*. Retrieved from http://www.eccouncil.org/Certification/ec-council-certified-incident-handler

EC-Council. (n.d.). *EC-Council certified incident handler course outline, Version 1*. Retrieved from http://www.eccouncil.org/portals/0/Images/img/icons/ECIH-v1-Course-Outline.pdf

Esposito, J.M. (2011). *New York City chief fire officer's evaluation of the citywide incident management system as it pertains to interagency emergency response* (master's thesis). Retrieved from the Homeland Security Digital Library.

Favero, G.T. (1999). *Flexibility of the incident command system to respond to domestic terrorism* (master's thesis). Retrieved from the Homeland Security Digital Library.

Federal Emergency Management Agency. (2012). *Emergency management institute: Independent study program* Retrieved from http://training.fema.gov/is/

Ferran, L. & Radia, K. (2013, July 9). *Edward Snowden: U.S., Israel 'co-wrote' cyber super weapons Stuxnet*. ABC News. Retrieved from http://abcnews.go.com/blogs/headlines/2013/07/edward-snowden-u-s-israel-co-wrote-cyber-super-weapon-stuxnet/

Fildes, J. (2010, September 23). *Stuxnet worm 'targeted high-value Iranian assets.'* BBC. Retrieved from http://www.bbc.com/news/technology-11388018

Givens, A. (2011, May 27). Deepwater Horizon oil spill is an ominous sign for critical infrastructure's future. *Emergency Management* Retrieved from http://www.emergencymgmt.com/disaster/Deepwater-Horizon-Oil-Spill-Critical-Infrastructure-052711.html?page=1&

How to get your CISSP certification. Retrieved from https://www.isc2.org/cissp-how-to-certify.aspx

. (2014b). *CISSP–professional experience requirement*. Retrieved from https://www.isc2.org/cissp-professional-experience.aspx

Jevis, E. (2014, January 13). *SU selected as a top military-friendly school*. Retrieved from http://news.syr.edu/su-selected-as-a-top-military-friendly-school-61362/

Katz, Y. (2010, December 15). Stuxnet virus vet back Iran's nuclear program by 2 years. *The Jerusalem Post*. Retrieved from http://www.jpost.com/Iranian-Threat/News/Stuxnet-virus-set-back-Irans-nuclear-program-by-2-years

Lam, C., Lin, M., Tsai, S., & Ta-Chiu, W. (2010). A pilot study of citizens' opinions on the incident command system in Taiwan. *Disasters*

Lutz, L.D. & Lindell, M.K. (2008). Incident Command System as a Response Model Within Emergency Operations Centers during Hurricane Rita. *Journal of Contingencies and Crisis Management*

Mississippi State University. (2014). Department of Computer Science and Engineering: Academics [Course listing]. Retrieved from http://www.cse.msstate.edu/academics/understud/

Mississippi State University. (2014b). Center for Computer Security Research [Course listing]. Retrieved from http://www.security.cse.msstate.edu/academics.php

Mississippi State University. (2013). Department of Computer Science and Engineering: Prospective Students. Retrieved from http://web.cse.msstate.edu/prospective/grad/msguidelines.php

Moynihan, D. P. (2009). The network governance of crisis response: Case studies of incident command systems. *Journal of Public Administration Research and Theory*

Moynihan, D. P. (2009b). From intercrisis to intracrisis learning. *Journal of Contingencies and Crisis Management*

Moynihan, D. P. (2008). Combining structural forms in the search for policy tools: Incident command systems in U.S. crisis management. *Governance: An International Journal of Policy, Administration, and Institutions*

Moynihan, D. P. (2007). *From forest fires to Hurricane Katrina: Case studies of incident command systems*. IBM Center for the Business of Government. Retrieved from the Homeland Security Digital Library.

National Security Archive. (2013, April 26). *Update: Agent Farewell and the Siberian pipeline explosion*. Retrieved from https://owl.english.purdue.edu/owl/resource/560/10/

Nemeth, E., Snyder, G., & Hein, T.R. (2010). *Unix and Linux system administration: 4th edition*. Upper Saddle River, NJ: Prentice Hall.

The 9/11 Commission. (2004). *The 9/11 Commission Report*. Retrieved from http://www.9-11commission.gov/report/911Report.pdf

Norwich University. (2014). BS in Computer Security and Information Assurance [Course listing]. Retrieved from http://profschools.norwich.edu/business/csia/curriculum/

Norwich University. (2014b). Information Assurance Minor [Course listing]. Retrieved from http://profschools.norwich.edu/business/csia/information-assurance-minor/

Ponemon Institute. (2014). *2014 best schools for cybersecurity* Retrieved from http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_2014_Best_Schools_Report.pdf

SANS Institute. (2014). GIAC Certified Incident Handler (CIH). Retrieved from http://www.giac.org/certification/certified-incident-handler-gcih

Symantec. (2012, December 18). *Security bulletin from SANS Institute*. Retrieved from http://www.symantec.com/connect/blogs/security-bulletin-sans-institute

Syracuse University. (2015). Academic Programs: Cybersecurity. Retrieved from http://eng-cs.syr.edu/prospective-students/academic-programs/masters/detail/cybersecurity

Syracuse University. (2015b). 2015–2016 Graduate Course Catalog: Certificate of Advanced Study in Information Security Management [Course listing]. Retrieved from http://coursecatalog.syr.edu/preview_program.php?catoid=4&poid=1521

Ullman, M. (1998). *Integration of the incident management system between the police and fire departments of the city of Goodyear, Arizona*. Retrieved from the Homeland Security Digital Library.

University of Texas at San Antonio. (n.d.). *UTSA Cyber Security* Retrieved from http://utsa.edu/cybersecurity/

University of Texas at San Antonio. (n.d.-b). Bachelor of Business Administration Degree in Cyber Security [Course listing]. Retrieved from http://www.utsa.edu/ucat/cob/bbaia.html

University of Texas at San Antonio. (n.d.-c). Master of Science Degree in Information Technology–Information Assurance Concentration [Course listing]. Retrieved from http://www.utsa.edu/gcat/chapter6/COB/istmdept.html#msitiac

University of Texas at San Antonio. (n.d.-d). Dependency graph of required CS courses and concentrations: 2014–2016 catalog. Retrieved from http://www.cs.utsa.edu/uploads/docs/CSCoursesForMajorsConcentrations_2014.pdf

University of Texas at San Antonio. (n.d.-e). Information Systems (IS) Course Descriptions. Retrieved from http://www.utsa.edu/ucat/cob/is.html#is3523

ICS-400: Advanced Incident Command System. Retrieved from http://www.vaemergency.gov/em-community/training/ics-400-advanced-ics-400

Warrick, J. (2011, February 16). Iran's Natanz nuclear facility recovered quickly from Stuxnet cyber attack. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html

Yates, J. (1999). Improving the management of emergencies: enhancing the ICS. *Australian Journal of Emergency Management*, Winter, 22–28.

Austen D. Givens adgivens@utica.edu) is an assistant professor of cybersecurity at Utica College and a doctoral candidate at King's College London. With Nathan E. Busch, he is the author of *The Business of Counterterrorism: Public-Private Partnerships in Homeland Security* (2014). Follow him on Twitter @GivensAD