THE CIP REPORT

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM VOLUME 5 NUMBER 7

January 2007

Department of Defense

Editorial Staff

Editors
Jeanne Geers
Jessica Milloy Goobic

Staff Writers
Amy Cobb
Maeve Dion
Colleen Hardy
Randy Jackson

JMU Coordinators
Ken Newbold
John Noftsinger

Publishing
Zeichner Risk Analytics

Contact: CIPP01@gmu.edu
703.993.4840
Click **here** to subscribe. Visit us online for this and other issues at http://cipp.gmu.edu

This month's issue of *The CIP Report* focuses on critical infrastructure protection in the Department of Defense. The DOD plays a complex and multi-layered role in relation to the protection of critical infrastructure/key resources, by not only serving as the Sector Specific Agency for the Defense Industrial Base, but also by being home to some of the most mature CIP programs of any department.

To that end, we are pleased to feature contributions from the Joint Task Force- Global Network Operations, which in support of the US Strategic Command (USSTRATCOM) and with guidance of the DoD CIP Draft Strategy, contributes to the overall vision, mission and goals of the Defense Critical Infrastructure Protection Program (DCIP). In addition, we also have an article from Dr. Dan Kuehl of the National Defense University's Information Resources Management College and a joint contribution from James Bret Michael of the Naval Postgraduate School and Duminda Wijesekera of George Mason University on their project "Secure Execution Framework for Active Coalition Partners in Maritime Domain Awareness." This issue also includes two articles from our own CIP Program Legal team, one providing an updated perspective on the Jose Padilla case, and the second providing an insightful overview of the role of the National Guard in disaster response and critical infrastructure protection.

As always, we hope you enjoy this issue and appreciate your continued support of the CIP Program. As we move into 2007, we continue to seek and present topics of importance to the CIP community and encourage all of our readers to bring contributions or topics of this nature forward for dissemination to the professionals within this field.

John A. McCarthy
Director, CIP Program
George Mason University, School of Law

Joint Task Force—Global Network Operations: The Agent of NetOps

In less than a decade, traditional Command and Control (C2) doctrines have evolved to include the concept of computer network-based operations. Within the Department of Defense (DoD), C2 now involves an environment dependent on the Global Information Grid (GIG), an enterprise whose operation and defense is the responsibility of a single functional component of United States Strategic Command (USSTRATCOM).

That component is the Joint Task Force—Global Network Operations (JTF-GNO). Its nascency can be traced to a series of real-world cyber events in 1997 that targeted DoD networks. Those events showed two things clearly: the vulnerability of DoD mission-essential computer assets, and the need for a single organization with the appropriate levels of authority for the GIG.

The JTF-GNO's mission is to "direct the operation and defense of the GIG to assure timely and secure net-centric capabilities across strategic, operational, and tactical boundaries in support of DoD's full spectrum of warfighting, intelligence, and business missions."[1] The JTF-GNO's Commander, who also serves as the Director, Defense Information Systems Agency (DISA), reports to the Commander, USSTRATCOM.

With the approval of a Joint NetOps Concept of Operations (NetOps CONOPS) in 2006, CDRUSSTRATCOM provided the common framework and C2 structure to combine the disciplines of enterprise systems and network management, network defense, and information decision management as outlined in the Unified Command Plan (UCP) 2006. This operational framework of essential tasks, situational awareness, and C2 is collectively known as NetOps.

In addition to that framework, the JTF-GNO—in support of USSTRATCOM and with the guidance of the DoD CIP Draft Strategy—augments the overall vision, mission, and goals of the Defense Critical Infrastructure Protection (DCIP) Program in accordance with DoDD 3020.40. The JTF-GNO also supports the CIP by working with the NetOps Community of Interest to identify, prioritize, and protect critical GIG assets required to enable Net-Centric capabilities and assure the availability of the GIG. The JTF-GNO's Component Commands within the Services have responsibilities for ensuring the availability of critical assets in support of the GIG. And with the GIG Sector, the JTF-GNO works to provide the accurate characterization and protection of the GIG. Those two organizations—JTF-GNO and the GIG Sector—are currently working to develop a GIG Criticality Methodology Process and the CIP Annex to the OPLAN 07-01 which will become the CIP Execution Document.

While the JTF-GNO's responsibilities are delineated in the NetOps CONOPs, the GIG Sector has the responsibility of characterizing those critical systems, functions, and assets that encompasses the GIG. GIG Sector is an organization that plans and coordinates with all DoD Components that own or operate supporting elements of the GIG to identify, analyze, and assess critical assets and related mission impacts, and collaborates with other Defense Sector Lead Agencies and DoD Components to identify cross-sector interdependencies.

As a construct, NetOps "relies on the understanding, application, and integration of information technology, technology standards, and standard processes that provide traditional systems and network management (Fault Management, Configuration Management, Accounting Management, Performance Management, and Security Management [FCAPS]); informa-

(Continued on Page 3)

JTF-GNO *(Continued from Page 2)*

tion and infrastructure protection; and the ability to maneuver information across GIG terrestrial, space, airborne and wireless environments."[2]

UNITED STATES STRATEGIC COMMAND

NetOps puts a combatant commander in charge of the GIG, end-to-end; it surpasses basic network management and computer network defense practices in net-centric military operations. NetOps includes not only balancing theater and Service equities, but establishing and sharing GIG situational awareness (SA) across the DoD. NetOps does not mean that network providers or frontline defenders relinquish their responsibilities for their respective Combatant Command, Service, or Agency; it does require that everyone synchronize their efforts to maximize efficiency, ensure data availability, and enhance protection of the network at large.

NetOps includes USSTRATCOM's operational responsibilities for Information Assurance (IA), Computer Network Defense (CND), Critical Infrastructure Protection (CIP) and other GIG defense tasks. NetOps is not intended to replace institutional practices of IA and CND, but to enhance them through a comprehensive process of protection, monitoring, detection, analysis and response.

Through the use of NetOps, directing the operation and defense of the GIG—with its thousands of applications and local area networks, sensors and circuits—can be effectively achieved. This end state—the effects that NetOps ultimately strives for—is an environment consisting of assured availability of both systems and networks, as well as assured delivery and protection of information. By bringing this balance of capabilities to the DoD's information environment, the JTF-GNO will unite all users of the GIG with common standards and processes, with potentially vast implications for mission success in all areas of the Department.[3]

Operating in this unique and dynamic area of responsibility, the JTF-GNO has command relationships with the Services, COCOMs, and DoD Agencies. Its mission partners also includes allied nations, other US Government Departments, the National Cyber Response Coordination Group (NCRCG), US Computer Emergency Response Team (US-CERT), law enforcement agencies, the Intelligence Community, and the private sector, including telecommunications, banking and finance, transportation, and the information technology industry.

Four overarching concerns govern the JTF-GNO's daily activities: who is on the network, what does the network look like, where are the vulnerabilities, and how can the risks be mitigated? The JTF-GNO addresses those concerns by serving as the fusion point for its mission partners, producing alerts, bulletins, Information Assurance Vulnerability Assessments (IAVAs), and Communication Tasking Orders (CTOs) to direct the operation of the GIG. In addition, JTF-GNO manages the status of Watch Condition (WATCHCON) and Information Condition (INFOCON), which govern the defensive tactics and policies users of the GIG need to follow.

As well as overseeing the day-to-day activities of the GIG, the NetOps CONOPS prepares the way ahead and strengthens the tools being brought to the fight.

According to the JTF-GNO Strategic Plan, the vision is to "lead an adaptive force that assures the availability, delivery, and protection of the GIG." The JTF-GNO – the Agent of NetOps – is helping to create the conditions on which net-centricity will succeed.

[1] NetOps Concept of Operations Version 3, August 4, 2006, p. 33.

[2] Ibid, p. 4

[3] JTF-GNO: Maturing Its Mission and Methods, unpublished manuscript by the Directorate for Strategy, Plans, Policy & International Relations (J5), JTF-GNO. ❖

The Role of the National Guard in Disaster Response and Critical Infrastructure Protection

Maeve Dion, Legal Research Associate, CIP Program

Last year, the media widely covered a dispute between state governors and the federal government regarding the President's authority to transfer National Guard members into federal status. However, less openly discussed was a general apprehension regarding the relatively undefined role of the National Guard in protecting critical infrastructure. This article summarizes these issues and presents various questions for debate.

The 2007 Defense Authorization Act

During the summer of 2006, governors expressed concerns regarding National Guard provisions in pending federal Defense Authorization legislation. As originally drafted, some of these provisions expanded the President's authority to call up Reserve members (including federalizing the National Guard) into active duty for the purpose of responding to natural or man made disasters or emergencies. These troops would shift from Title 32 status (under state governors' control) to Chapter 10 status (federalized).

There are many pieces of existing legislation that define when the President may federalize the National Guard, but in most circumstances the President does so only with the request or consent of the governors. However, under certain provisions, like the Insurrection Act, the President may call troops into active duty without such consent.

There are some limitations to this power, though. For example, under pre-2006 law, the President (1) could not call up Reserve members into active duty to perform functions authorized by the Insurrection Act; and (2) could not call up Reserve members into active duty to respond to "a serious natural or man made disaster, accident, or catastrophe," except in cases of threats or emergencies involving weapons of mass destruction (WMD) or terrorist attacks.

Gulfport, September 6, 2005 -- National Guard helicopters await delivery missions at the Gulfport, Miss. airport. *FEMA/Mark Wolfe*

In the Defense Authorization legislation drafted last year, both the House and Senate bills loosened these limitations to varying degrees. In the post-Katrina environment, the Congress wanted to make sure that the President's authority could reach the Reserve components in response to a natural disaster, or in response to an insurrection that resulted from the lawlessness following a natural disaster.

However, the state governors feared that if these provisions survived conference, the governors would lose flexibility in allocating state National Guard resources. Thus, during the conference of the House and Senate bills, the governors actively lobbied Congress to remove the provisions. At the same time, the Department of Defense insisted that maintaining its Total Force structure in the current post-9/11 military climate required Presidential authority to call up Reserves in support of both military missions and military responses to emergencies.

In deference to the concerns of the governors and the DoD, the Congress compromised, and with the final, conferenced, *John Warner National Defense Authorization Act*

(Continued on Page 5)

National Guard *(Continued from Page 4)*

for Fiscal Year 2007, the President has authority to call up the Reserve forces in support of military missions -- (1) Title 15 missions (Insurrections); (2) missions to put down invasion or rebellion, or if the President is otherwise unable "with the regular forces to execute the laws of the United States;" and (3) responses to emergencies involving a use or threatened use of a WMD, or a "terrorist attack or threatened terrorist attack in the United States that results, or could result, in significant loss of life or property."

The 2007 Defense Authorization Act revised the Insurrection Act (10 U.S.C. § 333) -- renaming it *Major Public Emergencies; Interference with State and Federal Law*, and openly acknowledging that, as long as the traditional (unchanged) legal requirements of the Insurrection Act were met, the President could invoke this authority even if the lawless situation resulted from an event or condition that may not comfortably fit the term "insurrection" (e.g., natural disaster, epidemic, terrorist attack, or other condition in which violence has occurred to such an extent that the state authorities can no longer maintain public order).

Therefore, with this new legislation, Congress removed the prior limitation on the Presidential authority to call up Reserve members into active duty to perform functions authorized by 10 U.S.C. § 333 (the former "Insurrection Act"). However, Congress retained the limitation that the President may not call up Reserve members into active duty to respond to disasters except in cases of threats or emergencies involving WMD or terrorist attacks. However, if a disaster (non-WMD and non-terrorism related) resulted in such lawlessness that the high legal threshold for invoking 10 U.S.C. § 333 was met (and this legal requirement was unchanged by the new legislation), then the President *may* call up Reserve members into active duty in response.

National Guard and CIP

While the 2007 Defense Authorization Act was still in conference, the CIP Program was asked to provide legal and policy analysis to advisors of some state governors. These discussions and analysis raised National Guard issues beyond the scope of the legislation. A review of the various federal policy statements, plans, and strategies provided only limited insight, and the governors have been occasionally frustrated in not receiving clearly defined, coordinated answers from the federal agencies.

In the event of a declared emergency / catastrophic incident, a governor does not want to lose his ability to prioritize and allocate his resources, particularly the state National Guard. The governor's priority is to use National Guard troops to help with broken levees along a major river. However, the DoD deems its priority to be the assignment of troops to guard certain critical infrastructure located in the state. Who has final decision-making authority in using the National Guard?

During domestic incidents, the DoD Secretary "shall retain command of military forces providing civil support." The DoD prefers to operate under the traditional, three-tier approach: (1) the DoD (as ordered by the President or DoD Secretary) provides support to local / Federal law enforcement; (2) the National Guard (as ordered by the state governor), performs homeland defense and homeland security activities; and (3) the US military (as ordered by the President or DoD Secretary) intercepts threats.

According to the DoD, certain authorities "under Title 32 of US Code -- and the National Guard's on-going transformation -- provide Governors and state authorities with the authority to use flexible, responsive National Guard units for a limited period to perform homeland defense activities, when approved by the Secretary of Defense. For example, National Guard forces may, when the Secretary of Defense determines that doing so is both necessary and appropriate, provide security for critical infrastructure and support civilian law enforcement agencies in responding to terrorist acts."

With its "Total Force" approach, the DoD recognized that one of the "most promising areas for employment of the National Guard and Reserve forces ... [is] Critical Infrastructure Protection, including the performance of comprehensive assessments of critical infrastructure sites and utilization of Reserve component forces for quick reaction requirements, when sufficiently trained and resourced, and local security at key defense and non-

(Continued on Page 14)

Legal Insights

Jose Padilla Case Update

Colleen Hardy
Senior Legal Research Associate , CIP Program

Although our Legal Insights column usually examines topics directly related to critical infrastructure protection, the upcoming trial of Jose Padilla presents a good opportunity to summarize the latest developments of a significant terrorism related case relevant to the field of homeland security.

Last February, I wrote an article describing Padilla's case. Padilla was detained as an enemy combatant in military custody in Charleston, South Carolina for three and a half years. Padilla was indicted in November 2005 in a Miami federal court on several charges. In January 2006, he was released from Department of Defense custody to Department of Justice custody in Miami to stand trial. Padilla pled not guilty.

Padilla's trial was originally scheduled to begin in the fall of 2006. However, while Padilla's trial was pending, his case has continuously made headlines.

US District Judge Marcia Cooke was assigned to Padilla's case. In March 2006, because special caution was necessary to prevent sensitive national security information from being released, Judge Cooke imposed strict constraints on the handling of classified material. For example, her order permitted Padilla's attorneys to examine secret evidence under special conditions. The following month, the United States Supreme Court denied Padilla's writ of certiorari. Padilla filed the writ after the Court of Appeals for the 4th Circuit determined Padilla's constitutional rights had not been violated by his detention. Justice Anthony M. Kennedy, writing for the majority, acknowledged Padilla's concern that there is a chance he may be placed back in Department of Defense custody. However, he reasoned Padilla's concern could be addressed when necessary, not while it was still hypothetical.

Padilla's defense attorneys argued the indictment contained minimal facts. In June 2006, Judge Cooke agreed and determined there was insufficient evidence concerning the allegations that Padilla and the other two co-defendants conspired to kill, injure or kidnap people overseas as part of a global Islamic terrorist network. She ordered federal prosecutors to provide additional evidence concerning those allegations. Moreover, Judge Cooke's order, among other things, required prosecutors to release the names of unindicted co-conspirators.

In a July 2006 order, Judge Cooke allowed Padilla to view classified documents and videotapes. The classified information contained statements Padilla made while he was detained at the South Carolina brig. According to one news report, defense lawyers in terrorism cases usually obtain security clearances, which enable them to view classified material. However, it is rare that the terrorist suspect is provided with direct access to such information. Judge Cooke's order grants Padilla with the opportunity to examine 32 Defense Department documents which summarize his statements. Cooke's order specified the details accorded to Padilla to review these documents: Padilla and his defense team will be placed in a secure room in the courthouse, the door must be kept open at all times and a US Marshall will be present, but placed "an appropriate distance" from the room to avoid hearing defense strategy. Furthermore, if the marshal does hear any defense details, he is prohibited from divulging such information to the government. As one news report stated, "The challenge in national security cases is in striking a balance between a defendant's right to prepare an adequate defense and the government's interest in protecting its secrets, particularly sources and methods used to obtain intelligence."

Later that month, a pretrial hearing was held to determine whether statements Padilla made to FBI agents at Chicago O'Hare airport in May 2002 should be admissible to his trial. Defense attorneys argued

(Continued on Page 7)

Legal Insights *(Continued from Page 6)*
Padilla was officially in law enforcement custody and unless he was advised of his Miranda rights, any statement Padilla made cannot be admissible at his trial. FBI Agent, Russell Fincher, testified at the hearing and stated Padilla was not read his Miranda rights until the end of the interview. Furthermore, Agent Fincher stated Padilla repeatedly agreed to talk to the agents, he was never handcuffed or restrained and he never asked to speak with an attorney.

In early August, after both defense counsel and federal prosecutors supported a delay to Padilla's trial, Judge Cooke reluctantly agreed to delay his trial until January 22, 2007.

On August 21, Judge Cooke dismissed one of the charges against Padilla and the other two defendants. Judge Cooke declared the conspiracy charge "to murder, kidnap and maim persons in a foreign country" repeated the other counts in the indictment. The prosecutors filed an appeal of Cooke's order with the 11th US Circuit Court of Appeals.

In early September, US Magistrate Judge Stephen Brown determined that Padilla's statements to FBI agents in May 2002 would be admissible at his trial. He declared that Padilla was not immediately placed under arrest and as a result he was not in official custody. Therefore, at that point Miranda warnings were unnecessary. Judge Brown stated "He was never told that he was not free to go." Therefore, Padilla's statements to FBI agents will be admitted to his trial. Judge Brown also determined that evidence seized from Padilla at the airport will also be admissible; this includes $10,000 cash and a cell phone allegedly given to Padilla by another al Qaeda operative. The phone allegedly contains the names of Padilla's al Qaeda recruiter and sponsor. Judge Cooke must review Judge Brown's decisions before the trial begins.

On September 14, Judge Cooke ordered the prosecution to release Padilla's medical records established while he was detained at the military brig. Cooke's order includes all physical and mental evaluations conducted on Padilla and all medication he took while he was at the brig. Defense attorneys requested the information to examine Padilla's treatment and to determine whether the government engaged in any misconduct during Padilla's detention. The prosecution argued the medical records did not have any relevance to the offenses filed against Padilla. Cooke disagreed with the prosecution and ordered them to release such records.

On October 7, Padilla's attorneys filed a motion to dismiss all charges against Padilla because of the "outrageous government conduct" while he was detained at the South Carolina military brig. Furthermore, they argued that due to the extensive length of time between the date of Padilla's arrest and his subsequent indictment and the mental trauma he suffered, he lacks the ability to defend himself. His attorneys claim, among other things, that Padilla: spent 1,307 days in isolation, was forced into painful stress positions, threatened with "imminent execution," kept awake for several days with bright lights and loud noises, and denied a copy of the Q'uran for almost two years. They also claim he was given a form of a "truth serum" drug, which may have been LSD or PCP. His attorneys did not provide any corroborating evidence or witnesses to support these allegations.

On November 13, federal prosecutors responded to Padilla's motion to dismiss and denied all claims that he was tortured while at the brig, insisting he was treated humanely. The prosecutors also argued that Padilla failed to provide any evidence to support these new allegations. As for the conditions of Padilla's confinement, the prosecutors argued they were humane and implemented to ensure his safety and security while detained at the brig. They argued Padilla received hala food, he was granted some outdoor exercise and he received medical attention when necessary.

Additionally, for the first time, the government disclosed the identity of the informants, Abu Zubaydah and Binyam Muhammad, who provided information for Padilla's material witness warrant. Both had previously been detained in an undisclosed CIA prison and were transferred to Guantanamo Bay in September 2006. According to the government's response, in early 2002, Zubaydah identified Padilla from a passport picture and told interrogators that Padilla and Muhammad were working together on a plot to detonate a radioactive "dirty bomb" in the United States. Muhammad stated he and Padilla researched the bomb together and received training in explosives wiring, but that al Qaeda leaders ultimately "directed

(Continued on Page 13)

Secure Execution Framework for Active Coalition Partners in Maritime Domain Awareness

James Bret Michael, The Naval Postgraduate School

Duminda Wijesekera, George Mason University

1. Introduction

Maritime Domain Awareness (MDA) is predicated on our domestic homeland defense and security communities, along with their foreign counterparts and nongovernmental organizations, maintaining a common intelligence picture (CIP) of maritime traffic via a distributed network of intelligence, surveillance, and reconnaissance (ISR) systems. MDA supports Maritime Domain Protection (MDP), which is to safeguard the security of the US and its allies; that is, MDA provides actionable intelligence information for use in conducting military, law enforcement and intelligence activities to protect against maritime-based threats to national security.

Context of the use of MDA at the summary level is as follows: To maintain a common intelligence picture of maritime traffic. The summary level can be decomposed into high-level user goals, with each goal associated with the MDA/MDP interdiction chain: detect, track, assign interdiction resources, engage interdiction-target, and assess engagement. To satisfy these user goals, MDA data and information will need to be exchanged amongst the primary actors in MDA/MDP. However, due to the sensitivity of certain MDA data and information, and the trust relationships between actors, controls on data and information flow will need to be formulated and maintained; that is, the control of data and information flow is a necessary capability for establishing and fielding a common intelligence picture in support of MDA. Our initial work on this flow for protecting the data and information comprising the MDA coalition common intelligence picture is being used by Navy Tactical Exploitation of National Capabilities (TENCAP) Radiant Alloy Program to support the development of access and flow controls for MDA intelligence collection and dissemination systems.

2. Project Summary

Our work builds upon the thesis research reported by LT Matt Tardy, USN and CPT Chris McDaniel, USA[1] on role-based access control for MDA, and that of LT Michael Bennett, USCG[2] on defining a common intelligence picture for MDA. In particular, we are investigating the technical feasibility of applying the following formal policy-based techniques in order to provide the level of system-wide trust and system dependability that will be necessary in order for actors involved in MDA to push and pull data from the common intelligence picture:

- Define the Unified Modeling Language (UML) use cases and actors for the MDA requirements. Actors are decorated with their trust levels so that the trust level of a use case can be estimated, and use cases parameterized by global variables (i.e., encoding the trust level, input/output data and others). Each use case has a goal and a collection of actors. An example goal is to intercept and confiscate any material usable to produce nuclear fuel that is transported without a permit. Thus, each use case has many actors, such as US Coast Guard personnel, harbormasters throughout the world, the Nuclear Regulatory Commission, informants, shipping companies, and foreign maritime agencies. Examples of global variables would be the time the material gets past the port of origin's customs services, the time it leaves the destination port's customs or is confiscated. The global use case can now be divided into a collection of local use cases (say divided upon regions of the sea covered by country or agency) that has the tasks of gathering information about vessels and their cargo, gathering information about permits issued to carry nuclear fuel, verifying the authenticity of submitted permits, and gathering

(Continued on Page 9)

MDA *(Continued from Page 8)*

information from the informants from other countries. Likewise, each local use case has to be divided into tasks (action sequences), where a use case is a synchronized (e.g., sequential or parallel) combination of tasks. Thus the tasks consisting of action sequences become goal-based plans of the objectives stated in the local use cases.

- Define the global metrics for a common intelligence picture, and global metrics for conducting MDP. To our knowledge, such metrics do not exist. We define them as computable functions of the input/output variables used in the tasks and actions that constitute the local use cases. However, global metrics for a common intelligence picture need to be developed in order to optimize use of resource. For example, the average time to report an incident is a global metric. Another global metric is the number of roles or organizations, or those that require human intervention to authorize an action. The objective is to distribute the resources so that it will maximize the global metric. In addition, those metrics can be used to identify the channels that facilitate the best information flows.

- Define foreseeable misuse cases [3, 4, 5, 6] (that would prevent the MDA use cases being executed) and a profile of potential mal-actors with estimated probabilities of their acting as predicted. Each misuse case has a potential mal-actor, and collection of misuse-cases can be a collaborative misuse case: these model groups of collaborating mal-actors and ways in which they could collaborate.

- Develop some attribute-based mis-roles (i.e. a way to specify potential role players in abusing a role-based access control system) that can be used to map the MDA/MDP use case/misuse case models to the role-based access control (RBAC) model developed by McDaniel and Tardy [1]. In order to do so, we propose to develop enhanced role based access control models in a non-trivial way as described below:

Specifying positive (i.e., directly useful) and negative (i.e., hindering) information with respect to achieving a specified objective can be used to model access and flow control. Such models have been developed at the specification level – named misuse cases. What is missing is their incarnation in role-based access control (RBAC) models that specify roles (i.e., duties that facilitate an organization to function as required) and what we name mis-roles: sets of duties that when executed would hinder the functionality of specified roles. Mis-roles in this context would profile typical destructive behavior from a security standpoint and therefore allow one to account for foreseeable attacker behavior during the design of an RBAC system. We have introduced mis-roles into RBAC, in addition to categorizing mis-behavior profiles based on their severity to the functionality of the organization. The immediate use of this in MDA is that any individual behavior that fits these legal but unwelcome behaviors can be tracked by the access controller.

James Bret Michael can be reached at (831) 656-2655 or bmichael@nps.edu. Duminda Wijesekera can be reached at (703) 993-1578 or dwijesek@gmu.edu.

References

1. McDaniel, C. R. and Tardy, M. L. Role-Based Access Control for Coalition Partners in Maritime Domain Awareness, master's thesis, Naval Postgraduate School, Monterey, Calif., June 2005.
2. Bennett, M. E. Defining a Common Intelligence Picture for the United States Coast Guard: A Port Perspective, master's thesis, Joint Military Intelligence College, Aug. 2003.
3. Sindre, G. and Opdahl, A. L. Eliciting Security Requirements by Misuse Cases, in Proc.TOOLS Pacific, Sydney, Australia, Nov. 2000, pp. 120-131.
4. Sindre, G. and Opdahl, A. L. Templates for Misuse Case Description, in Proc. 7th Int. Workshop on Requirements Engineering, Foundation for Software Quality, Interlaken, Switzerland, June 2001.
5. Alexander, I. Use/Misuse Case Analysis Elicits Non-Functional Requirements, Technical Report, 2002. http://easyweb.easynet.co.uk/~iany/consultancy/misuse_cases/misuse_cases.htm
6. Dwaikat, Z. and Parisi-Presicce, F. From Misuse cases to Collaboration Diagrams in UML, in Proc. 3rd Int. Workshop on Critical System Development with UML, Lisbon, Portugal, Oct. 2004, pp.130-138. ❖

Infrastructures, Protection, and [Future] Warfare

Dr. Dan Kuehl*
Information Resources Management College
National Defense University

Infrastructures have been important to national security for a very long time. The Romans, for example, had at least two that were vital to their economic, political, and military security and stability: water and transportation, most visible in the form of the networks of aqueducts and roads that encircled the Roman Empire. These systems enabled the growth of Roman cities, the stability of Roman society, the expansion of commerce across the entire Mediterranean region, and the ability to deploy Roman military power quickly (for that era) and to sustain it in the field. The American concept for strategic airpower in World War II, Billy Mitchell's "industrial web," was a form of infrastructural warfare, and this strategic concept was clearly visible in US air operations throughout the 1990s, against both Iraq and Serbia.[1] What is critical to any particular society depends on the details of that society and the specifics of its economic, political and military systems.[2] What is dramatically new, however, is the growing use in dozens of countries of interconnected computer systems to monitor the status and control the operations of these infrastructures, a capability that rests on widespread and growing reliance on systems employing SCADA--"supervisory control and data acquisition"—technologies which allow us to monitor the status and control the operation of a segment of infrastructure such as a rail network or an electric grid. Nearly any and every capability that supports strategic military, economic, and societal strength is linked together in this manner and depends on the smooth and uninterrupted functioning of ICT—"information and communications technologies"—to keep flowing whatever is needed, whether that be electricity, money, a trainload of tanks on their way to a port of embarkation, an air traffic control system, or one of a thousand other critical functions that support and enable all of the different elements and instruments of national power.

> ***In 1943 it took enormous physical and moral courage for American airmen to battle their way for several hours across very hostile skies to strike their targets, but now a similar effect might be achievable in a matter of seconds across intercontinental distances from a setting where the most immediate danger is acute eyestrain.***

This revolution has changed both WHAT an attacker might wish to attack as well as HOW it could be attacked and WHO might need to partner in its defense. Going back to the WW II model, the means of attacking German industrial infrastructures was massed airpower: hundreds or even thousands of bombers smothering a key target—an oil refinery, or electric generating plant, for example—with hundreds or even thousands of tons of high explosive.[3] With proper planning, adequate force, and some luck, sufficient explosive would be delivered to effectively destroy the target so that tomorrow's mission could go on to the next critical target and thus sequentially bring the infrastructure to collapse.[4] The focus on command and control systems and nodes that was highlighted by the American concept of "Command and Control Warfare—C2W" in the early 1990s--also had its origins in previous wars and campaigns. British General Edward Allenby's 1918 Palestine Offensive is just one prominent example, in which he feinted one way to get the Turkish forces out of position (military deception), carefully concealed the evidence of this maneuver (op-

(Continued on Page 11)

**The opinions contained herein are those of the author and should not be construed as those of the US Government, Department of Defense, National Defense University, or George Mason University.*

Kuehl *(Continued from Page 10)*

erational security or OPSEC) then used his airpower to strike and destroy the Turkish telegraph nodes along the railroad (CNA) to degrade the Turks' ability to effectively react to the disaster that was enfolding them.[5] The key addition to this mix of potential targets has been the control mechanism or even software itself, and the growing reliance on SCADA systems has added a new target category to the list of potential targets in strategic warfare.[6] Thus the informationized transformation of warfare has seen us evolve from attacking an infrastructure's physical components to perhaps attacking its informational components instead.

The next step in this transformation focuses on HOW we might attack those components. We understand and have a lengthy history of/experience with ways to physically attack these infrastructures, such as the WW II examples discussed above. But a "computer network attack" on the control systems for an enemy airspace control network would not require the massed forces of WW II, nor perhaps even the solitary and precise attacks of Desert Storm. Instead, it might only require a handful of people—who might not even need to be on the same continent, let alone in the same room—with powerful computer systems and software "weapons" who could cause the simultaneous disruption and even collapse of critical enemy systems, networks and capabilities.[7] In 1943 it took enormous physical and moral courage for American airmen to battle their way for several hours across very hostile skies to strike their targets, but now a similar effect might be achievable in a matter of seconds across intercontinental distances from a setting where the most immediate danger is acute eyestrain. But there are still many unresolved issues surrounding this new and unproven capability. Some of them are legal and ethical, and center on questions such as whether a virtual and non-kinetic cyber "attack" crosses the thresholds of "armed attack and aggression," in the language of the UN Charter. Others involve whether cyberspace has borders that can be crossed and violated, and if so, where are they? Another set concerns the status of those persons conducting the attack: are they criminals, or mercenaries, or uniformed combatants subject to the restrictions and protections of the "Law of Armed Conflict"? Although vigorous and sometimes sensitive debate has taken place within the highest levels of the defense establishment in the US and elsewhere, these issues remain unresolved.[8]

The third focus of this transformation is defensive: WHO is responsible for and capable of protecting and defending our own critical infrastructures against such threats? This is very much an evolving interagency question in which all levels of government—including regional and local—as well as the private sector's business community must be totally involved. Our existing paradigms for national security have been shaped by the battlespaces in which we operate, but the emergence of cyberspace is already complicating this.[9] The critical infrastructures discussed previously are almost exclusively owned and operated by the private sector—they are business enterprises. Who has the responsibility for securing the operation of these infrastructures and protecting their key assets and functions? Although both government and business acknowledge that the owners bear this responsibility, there is one exception: the uniformed military is responsible for the defense of the nation from enemy attack via the air, or land, or sea, or even outer space….but what of cyberspace? The US Air Force defends the elements of the Northeast Electric Grid against an attack using bombers…but who defends it against an attack using electrons and malevolent bits and bytes? Segments of the US business and government have been studying this issue for more than a decade, but this "roles and missions" debate is just beginning.[10] Critical national infrastructures cannot be adequately and effectively protected without the integrated and cooperative action of business and government, but these efforts are still underway.

(Continued on Page 12)

Dr. Kuehl teaches military strategy and national security policy in the Information Resources Management College at the National Defense University in Washington, DC. He teaches three of the four courses comprising the Information Operations Concentration, a specialized curriculum on the strategic employment of the information component of national power, offered annually to several dozen selected students at the National War College and Industrial College of the Armed Forces. His areas of expertise include national security in the information age, the law of war, the strategic use of the internet, public diplomacy, strategic communication, and information warfare and operations. He retired as a Lieutenant Colonel in 1994 after nearly 22 years active duty in the USAF.

Kuehl *(Continued from Page 11)*

We may have to wait until someone decides "the time is right" to make a strategic attack on these infrastructures, probably as an adjunct of a serious geostrategic crisis: finding out then that our interagency efforts have been ineffective might be the cyber equivalent of realizing on Monday, December 8, 1941 that you can drop aerial torpedoes in shallow-water harbors.[11]

Dr Dan Kuehl can be reached at kuehld@ndu.edu.

[1] This emphasis on attacking (or defending) specific nodes that could degrade entire systems can be seen as early as the first German daylight raid on London in 1917, in which facilities such as banks and railroad centers were intended targets. Air Force Colonel John Warden may have best captured this concept with his 1994 article on "The Enemy as a System" (*Air Power Journal*, Spring 1995; available electronically at http://www.airpower.maxwell.af.mil/airchronicles/apj/warden.html)

[2] The initial American strategic policy for CIP, Presidential Decision Directive (PDD) 63, issued by President Clinton in 1998, listed six critical infrastructure sectors (telecommunications, energy, banking and finance, transportation, water systems and emergency services); the new (2006) National Infrastructure Protection Plan (NIPP) has extended this to between 17 and 20, which is almost certainly too many. See http://www.fas.org/irp/offdocs/pdd/pdd-63.htm for an electronic copy of PDD 63; the Bush Administration expanded this list in Homeland Security Presidential Directive (HSPD) 7, available electronically at http://www.fas.org/irp/offdocs/nspd/hspd-7.html . The NIPP is available at the Department of Homeland Security's website http://www.dhs.gov/dhspublic/display?content=5476

[3] The oft-cited American concept for "precision high-altitude strategic bombardment" is often interpreted as the precision of the bombing, but the reality is that it was tremendously inaccurate in the aggregate: the precision was in the ability to destroy a specific target or facility. In a superb article comparing USAAF and RAF bombing accuracy, W. Hays Parks showed that on a bomber-by-bomber comparison, the RAF was more accurate, although this was more a factor of tactical doctrine and the need to operate in massed formations during daylight for self-protection against German air defenses. What WAS precise was the USAAF's ability--repeatedly demonstrated--to hit and destroy specific industrial installations and thus degrade and eventually fatally weaken Germany's industrial infrastructure. See John Gooch, editor, *Airpower: Theory and Practice* (London: Cass, 1995), especially W. Hays Parks "'Precision' and 'Area' Bombing: Who Did Which, and When", and Daniel T. Kuehl, "Airpower vs. Electricity: Electric Power as a Target for Strategic Air Operations".

[4] There is neither time nor space here to explore concepts such as "sequential" or "parallel warfare", which have been at the heart of the airpower debates within American and global defense circles since the Gulf War of 1991, but they are embedded deeply within concepts such as Information Warfare, Decision Superiority, and Command and Control Warfare. See Merrick Krause's short piece "Decision Dominance: Exploiting Transformational Asymmetries" for a short overview of some of these concepts. Available electronically at http://www.ndu.edu/inss/DefHor/DH23/DH_23.htm

[5] For a short but succinct description see Sir Basil Liddell hart's classic *The Real War, 1914-1918*, esp. pp.439-448. What General Allenby did was to get well inside of his opponent's "decision cycle" and thus serves as a wonderful example of what Colonel John Boyd called the "observe-orient-decide-act" or OODA Loop. For a short description of the OODA Loop concept see http://www.valuebasedmanagement.net/methods_boyd_ooda_loop.html ; for a longer examination and analysis of John Boyd's work see either of the two recent biographies of Boyd, Robert Corum's *John Boyd: the Fighter Pilot Who Changed the Art of War* (Little-Brown, 2002), or Grant Hammond's *The Mind of War: John Boyd and American Security* (Smithsonian, 2001). In this discussion the acronym CNA stands for "communications network attack", which is of course the same acronym used by Joint IO Doctrine for "computer network attack."

[6] SCADA can be defined as "a computer system for gathering and analyzing real time data. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation. A SCADA system gathers information, such as where a leak on a pipeline has occurred, transfers the information back to a central site, alerting the home station that the leak has occurred, carrying out necessary analysis and control, such as determining if the leak is critical, and displaying the information in a logical and organized fashion. SCADA systems can be relatively simple, such as one that monitors environmental conditions of a small office building, or incredibly complex, such as a system that monitors all the activity in a nuclear power plant or the activity of a municipal water system." See http://www.webopedia.com/TERM/S/SCADA.html for this definition and a list of additional links to the term; a Google search of it produced over 700,000 hits!

[7] For a perceptive—and perhaps frightening—set of non-US perspectives on this see several of the chapters in Mike Pillsbury, editor, *Chinese Views of Future Warfare* (Washington DC: NDU Press, 1997), especially Wang Pufeng "The Challenge of Information Warfare", Wang BaiBaocun & Li Fei "Information Warfare", and Wei Jincheng "Information War: a New Form of People's War", available electronically at www.ndu.edu/inss

[8] There is a growing body of literature on these topics, too extensive to cite completely here. The three best books are probably Walter Gary Sharp, *Cyberspace and the Use of Force* (Aegis Research: Falls Church, VA, 1999); Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace* (Aegis Research: Falls Church, VA: 2000); and Michael N. Schmitt and Brian T. O'Donnell, editors, *Computer Network Attack and International Law* (Naval War College: Newport RI, 2002); in the journal literature William Bayles' "The Ethics of Computer Network Attack" is good, in *Parameters* (Spring, 2001); available electronically at http://carlisle-www.army.mil/usawc/Parameters/01spring/bayles.htm

[9] The definition I use for cyberspace ("Cyberspace is an operational domain characterized by the use of electronics and the electromagnetic spectrum to create, store, modify and exchange information via networked information systems and telematic infrastructures") is very similar

(Continued on Page 15)

Legal Insights *(Continued from Page 7)*
Padilla to return to the United States to conduct reconnaissance on behalf of al Qaeda within the United States." Padilla's defense attorneys argued the evidence should not be admitted because, among other things, the informants may have been tortured and statements made under such conditions are not admissible. The government denies all allegations of torture.

In early December, still video images of Padilla were released to the public. These images depicted Padilla wearing chains, headphones and blacked out goggles. Padilla's attorneys filed these images with the court to strengthen their argument that all charges against Padilla should be dismissed. They claim the image illustrates how Padilla was detained at the brig and such detention amounts to torture. Padilla's attorney did not provide any background information concerning the image, but according to the New York Times, the image was taken as Padilla was being taken out of his cell for a dental procedure. Padilla's defense attorneys also included an affidavit from Dr. Angela Hegarty, a psychiatrist who met with Padilla a few times. According to her affidavit, she stated that Padilla suffers from post-traumatic stress disorder and as a result he is unable to adequately prepare for his defense.

The government responded to the images of Padilla. In a court document, federal prosecutors stated "Far from proving any abuse, these photographs highlight the absurdity of Padilla's assertion: namely that the United States was callous enough to mistreat Padilla while conscientious enough to tend to his toothache." They also argued that Padilla never reported any abusive treatment to the staff or medical personnel at the brig.

On December 19th, Judge Cooke ordered a mental evaluation for Padilla to determine whether he was competent to stand trial. Both prosecutors and defense attorneys agreed that Padilla's ability to understand the legal proceedings and assist his attorneys must be determined before his trial can begin.

On January 5, 2007, Judge Cooke provided prison officials another week to complete their mental examinations of Padilla to determine if he was competent to stand trial. The Bureau of Prison officials requested a longer period of time because Padilla was not "compliant with psychological testing" and as a result he had to be observed by staff members to complete the evaluation. Judge Cooke gave the officials another week to observe Padilla and ordered them to provide their report to the court by January 16. Cooke was adamant that their report be complete prior to the 22nd trial date so she could rule on other pending issues.

On January 8, Padilla's attorneys asked Judge Cooke to bar statements Padilla made while detained at the military brig from his trial. His attorneys argued the government cannot use his statements because they were coerced by the interrogators at the brig. That same day, federal prosecutors asked Judge Cooke to reconsider her deadline for the Bureau Prison official's mental examination report on Padilla. In their motion, the prosecutors argued, "The deadlines set out by the court may negatively affect the examination process and may prejudice the government's ability to demonstrate the fallacy of Padilla's competency allegations as well as the court's ability to make adequate findings, subject to appellate review, regarding this issue."

On January 10th, the 11th US Circuit Court of Appeals heard arguments concerning whether or not to reinstate the charge of conspiracy to "murder, kidnap and maim persons in a foreign country" against Padilla. This was the only charge filed against Padilla that carried a possible life sentence. Judge Cooke stated she will not begin Padilla's trial until the Court of Appeals settles this issue.

On January 12, Judge Cooke ordered a three month delay for Padilla's trial. Padilla's trial is now scheduled to begin on April 16.

As previously reported, four other men were charged with Padilla: Adham Amin Hassoun, Kifah Wael Jayyousi, Mohamed Hesham Youssef, and Kassem Daher. However, only two defendants will stand trial with Padilla: Hassoun and Jayyousi. The other two defendants are in custody overseas. ❖

National Guard *(Continued from Page 5)* defense critical infrastructure sites, when directed."

During discussions of the 2007 Defense Authorization Act, the governors posed this hypothetical: In the event of a declared emergency / catastrophic incident, a governor does not want to lose his ability to prioritize and allocate his resources, particularly the state National Guard. The governor's priority is to use National Guard troops to help with broken levees along a major river. However, the DoD deems its priority to be the assignment of troops to guard certain critical infrastructure located in the state. Who has final decision-making authority in using the National Guard?

The answers to this hypothetical depend on many factors, including which critical infrastructure assets the DoD wants guarded.

While the Department of Homeland Security is the Lead Agency for prevention, preparation, and response relating to domestic disasters and emergencies, the DoD is explicitly authorized to implement plans to protect the "defense industrial base," and the DoD is the lead agency for "homeland defense," which includes "defense critical infrastructure."

There is yet no clear definition as to precisely what portions of the Critical Infrastructure / Key Resources (CI/KR) fit into the these terms, or as to how much of the supply chain falls within the definitions.

In the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (White House, 2003), the defense industrial base is broadly defined as the "DoD and the private sector defense industry that supports it" (e.g., manufacturers of military equipment, materials, and weaponry; utilities that service military installations; etc.). The DoD defines the defense industrial base as "a worldwide industrial complex with capabilities to perform research and development and design, produce, and maintain military weapons systems, subsystems, components, or parts to meet military requirements."

Gulfport, September 5, 2005 -- Members of the Maryland National Guard pass out water and ice to residents of Gulfport, Miss. *FEMA/Mark Wolfe*

In its *Strategy for Homeland Defense and Civil Support* (2005), the DoD defines defense critical infrastructure as "DoD and non- DoD cyber and physical assets and associated infrastructure essential to project and support military forces worldwide. ... [D]efense critical infrastructure could also include selected civil and commercial infrastructures that provide the power, communications, transportation, and other utilities that military forces and DoD support organizations rely on to meet their operational needs." The DoD noted that protection of "critical defense assets [that] are located at public or private sites beyond the direct control of DoD ... must be assured on a priority basis."

The DoD has said that the President or DoD Secretary "might direct US military forces to protect non-DoD assets of national significance that are so vital to the nation that their incapacitation could have a debilitating effect on the security of the United States." This situation is envisioned "where the nature of the threat exceeds the capabilities of an asset owner and civilian law enforcement is insufficient."

In light of these definitions and statements, several questions remain:

1. How broadly should "defense critical infrastructure" and "defense industrial base" be defined?

2. What are the non-defense CI/KR "of national significance" such that the President or DoD Secretary may order US military forces (and National Guard) to protect them?

3. What is the role of the National Guard in protecting defense CI/KR and non-defense CI/KR? May a state governor use National Guard troops (in Title 32 status, not federalized) to perform homeland defense activities without the approval of the DoD Secretary (this question may merely relate to whether approval is needed only in the case of using Federal funding, or may be a deeper concern)? What kind of activities

(Continued on Page 15)

Kuehl *(Continued from Page 12)*
to the definition just published by in the National Military Strategy for Cyberspace Operations, and in fact was the basis for that definition. We have evolved to where military operations are now conducted in five physical media: air, land, water, outer space, and cyberspace. See my two 1997 "Strategic Forum" pieces on "Defining Information Power" and "Joint Information Warfare" (www.ndu.edu/inss) for a fuller explanation. I teach my students at the National Defense University that one critical way of looking at "jointness" is not the traditional combination of Services (Army, Navy, etc) but rather the integration of operational and warfighting environments cited above.

[10] This is hardly a US-only item of strategic interest: at least a dozen other countries have taken on this issue as vital to their national security. An excellent starting resource are the fine survey and analysis books published in Switzerland, *International CIIP [Critical Information Infrastructure Protection] Handbook 2004: An Inventory and Analysis of Protection Policies is Fourteen Countries* (Swiss Federal Institute of Technology: Zurich, 2004); available electronically at http://www.isn.ethz.ch/crn/publications/publications_crn.cfm?pubid=224 . Also see their newest study, published in 2006, which extends the analysis to 20 countries and several international organizations. An excellent starting point within the US was the publication of the findings of the President's Commission on Critical Infrastructure Protection (PCCIP or Marsh Commission, named after its head, Robert Marsh), *Critical Foundations* (available electronically at http://www.tsa.gov/interweb/assetlibrary/Infrastructure.pdf) in 1997. This was not only the key source document for President Clinton's PDD 63; it served the same role for efforts in several other countries. For the results of a symposium in which this topic of the shared roles of the partnership see Carolyn Pumphrey, editor, *Transnational Threats: Blending Law Enforcement and Military Strategies* (Carlisle PA: Army War College Strategic Studies Institute, 2000), especially Daniel T. Kuehl "The National Information Infrastructure: the Role of the DOD in Defending it", available electronically at http://www.carlisle.army.mil/ssi/pdffiles/PUB224.pdf

[11] One of the earliest—and still best—books on this entire set of issues is Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Boston: MIT, 2001). ❖

National Guard *(Continued from Page 14)*
fall into the "homeland defense activities" category? When should the National Guard move from state to Federal status in order to provide "homeland defense" (without domestic law enforcement capabilities) under the DoD?

4. How is such protection and planning coordinated among the state governors, DoD, DHS, and President?

As federal agencies in Washington, DC are actively attempting to define their roles and interrelationships (CIP, homeland defense, homeland security, etc.), the states are reaching out for similar levels of communication. As seen by the governors' active response to the draft National Guard provisions in the 2007 Defense Authorization Act, the states are an integral part of this kind of planning.

The questions posed in this article, and many more, are thus up for debate not only between the federal agencies but also between the states and federal government. Some of the answers and definitions are fluid, and criticality of an asset may depend on the circumstances. However, emergency preparedness requires a certain level of common understanding and categorization so that, for example, a governor may plan for the prioritization and allocation of state resources -- including the National Guard. Yet if the governor's plan conflicts with the DoD's priorities, and the conflict is not discovered until the emergency is already occurring, not only is the state response plan unexpectedly skewed, but the emergency situation may be worsened as a result. ❖

The CIP Program is directed by John A. McCarthy, a member of the faculty at George Mason University School of Law. The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the nation's critical infrastructure. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC (ZRA) on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for ***The CIP Report***, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1