Joint Doctrine Provides the Principles Required for the Science of Security Cyber Ecosystem

R. Zager 19 August 2015

This forum proposes to establish Semantic eScience as the scientific foundation for the cyber ecosystem. The author observes on p 42, "Just like we need infrastructure in areas like Meteorology to understand and predict the weather we need operational cybersecurity science infrastructure to understand and predict events in our cyber ecosystem of the future." In Meteorology, like other physical phenomena, nature takes its course irrespective of the observers. Semantic eScience adopts the independence of the observed and the observer, proposing an ecosystem in which people play a single role - people make future predictions based on observations of past events. This ecosystem excludes two key human groups – attackers and users.

Unlike forces of nature, attackers observe the actions of defenders and adjust in order to defeat the actions of the defenders. To the extent that past actions are predictive of future outcomes, attackers make changes to evade defenses. See, for example, RAND's The Defender's Dilemma: Charting a Course Toward Cybersecurity, http://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1024/RAND_RR1024.pdf

Unlike nature, "cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines." (Dr. Frederick Chang, former NSA Director of Research).

Users add more human interactions to the system by engaging in counterproductive security behaviors which can be are exploited by attackers. These behaviors include poor password practices, Shadow IT and falling victim to social engineering attacks. Security personnel often act on the false assumption that users will follow IT security instructions, security stubbornly refusing to admit that non-complaint users are the norm, not exceptions. See, for example, Kirlappos, et al., "Comply or Die" Is Dead: Long Live Security-Aware Principal Agents, Financial Cryptography and Data Security, Lecture Notes in Computer Science Volume 7862, 2013, pp 70-82.

Instead of a system in which one group of people make defensive decisions based on the Activity/Object matrix set forth on Page 39, there are three groups of people interactively making decisions –

- Analysts (the people envisioned in Semantic eScience)
- Attackers
- Users

There is an existing body of knowledge that addresses adversarial engagements and interactive human decision-making. That body of knowledge is Joint Doctrine. Joint Doctrine documents the accumulated insights and wisdom gained by the U.S. military from its adversarial engagements. Joint Doctrine is published at http://www.dtic.mil/doctrine/new_pubs/jointpub.htm.

Applying Joint Doctrine to the Science of Security, it is apparent that the attacker is applying intelligence (JP-2-0) using cyberspace operations (JP 3-12(R)) in an information operation (JP 3-13) targeting users and analysts by implementing information operations intelligence integration (IOII, JP 2-0, JP 3-13) for the purpose of espionage. A key tool in this operation is deception (JP 3-13.4). Analysts are applying intelligence (JP 2-0). The pivotal role of people making decisions is the reason that JP 3-13, *Information Operations,* identifies the human mind, not data sets, as the most important factor in information operations. Ultimately the adversary that will prevail is the one that has the faster decision and execution cycles which are based on better information – a core precept of JP 2-0, *Intelligence*.

Applying the 7 core themes demonstrates how Joint Doctrine provides a better approach to the Science of Security than Semantic eScience.

Common Language. Joint Doctrine provides a common language which is used by:

The President
The National Security Council
The Congress
The Department of Defense
The Defense Intelligence Agency
The National Security Agency
The National Geospatial Intelligence Agency
The National Reconnaissance Office
Army Intelligence
Navy Intelligence
Air Force Intelligence
Marine Corps Intelligence
The Central Intelligence Agency
The Department of State
The Department of Energy
The Federal Bureau of Investigation
The Department of the Treasury
Coast Guard Intelligence
The Department of Homeland Security
The Drug Enforcement Administration
The Office of Director of National Intelligence

By deviating from the definitions of the Joint Publications, Semantic eScience introduces unnecessary confusion into the discussion and analysis of cybersecurity. For example, comparing the models of understanding of Semantic eScience and the Joint Publications shows fundamentally different approaches and language.

Semantic eScience

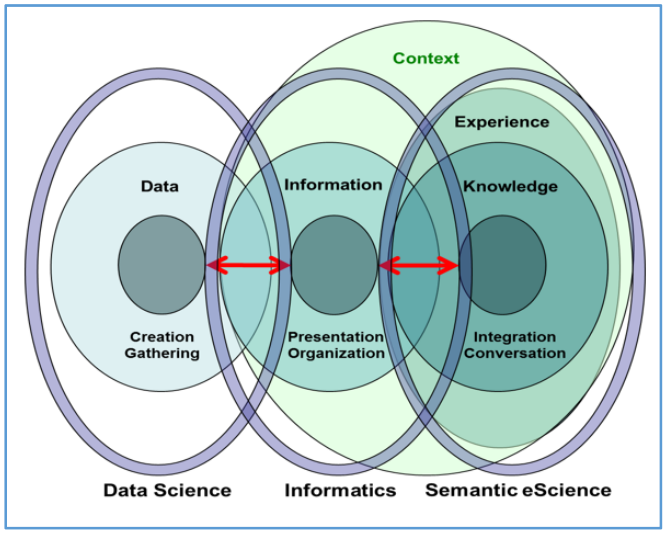


Figure 1

JP 2-0, *Joint Intelligence*

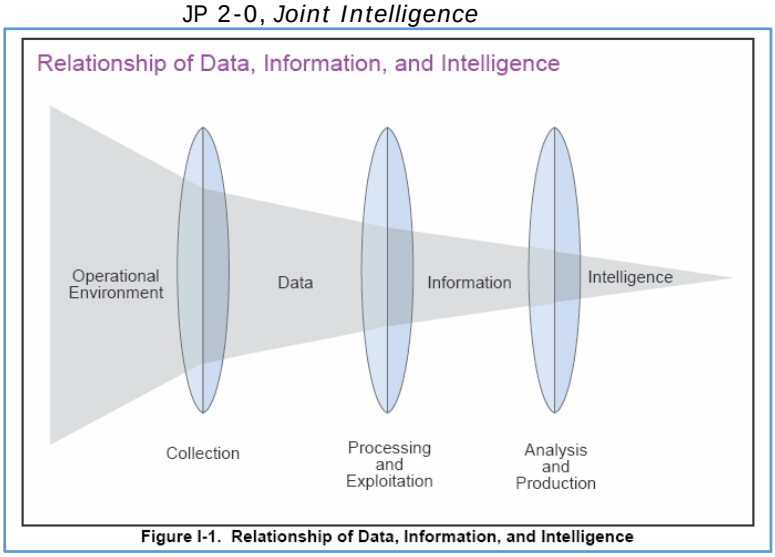


Figure I-1. Relationship of Data, Information, and Intelligence

Figure 2

The work product of Semantic eScience is Semantic eScience, the characteristics of which are data processing information. The work product of *Joint Intelligence* is intelligence. JP 2-0, *Joint Intelligence,* observes:

Ultimately, intelligence has two critical features that distinguish it from information. Intelligence allows anticipation or prediction of future situations and circumstances, and it informs decisions by illuminating the differences in available courses of action (COAs).

Semantic eScience uses the term "intelligence" to describe data sets. Data sets are "information" in the terminology of the Joint Publications. The different meanings of the term "intelligence" in the two frameworks is seen in last sentence of Paul Patrick's "Blueprint of a Semantic eScience of Security Technology Stack" https://www.linkedin.com/pulse/blueprint-semantic-escience-security-technology-stack-paul-patrick in which he uses the phrase "threat intelligence" to describe a data set which may or may not be predictive of future situations. "Threat Intelligence" is not a category of intelligence products in the Joint Publications.

"Intelligence" is merely one example of a divergence between current practice and the Semantic eScience proposal. If the Science of Security were to adopt Semantic eScience, the Science of Security

will diverge from the language and framework used by the U.S. Government, creating a body of knowledge that will not be readily usable by the U.S Government. All participants in cybersecurity would be well-served by a unified lexicon.

Rather than a new language, the Science of Security should use the definitions of the Joint Publications, making suggested amendments as is required.

Core Principles. Leveraging a system of metrics to align solutions and data collection is a concept already incorporated in Joint Doctrine. The Core Principles most closely aligned to cybersecurity are set forth in JP 2-0, *Joint Intelligence*, and JP 3-12(R), *Cyberspace Operations*.

Attack Analysis. The Attack Analysis of the Semantic eScience system suffers from too narrow a focus, looking merely at the data artifacts. We see this in a side-by-side comparison of the Semantic eScience model to the three dimensions of the Information Environment set forth in JP 3-13, *Information Operations*:

Semantic eScience

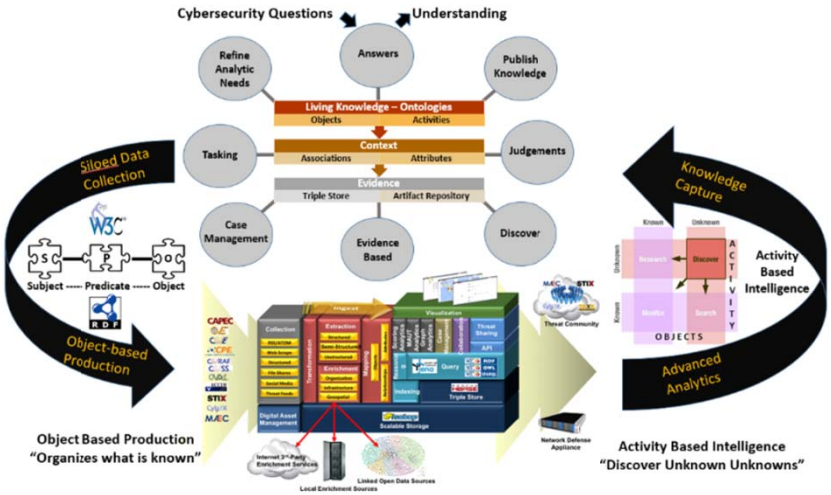


Figure 3

JP 3-13 Information Operations

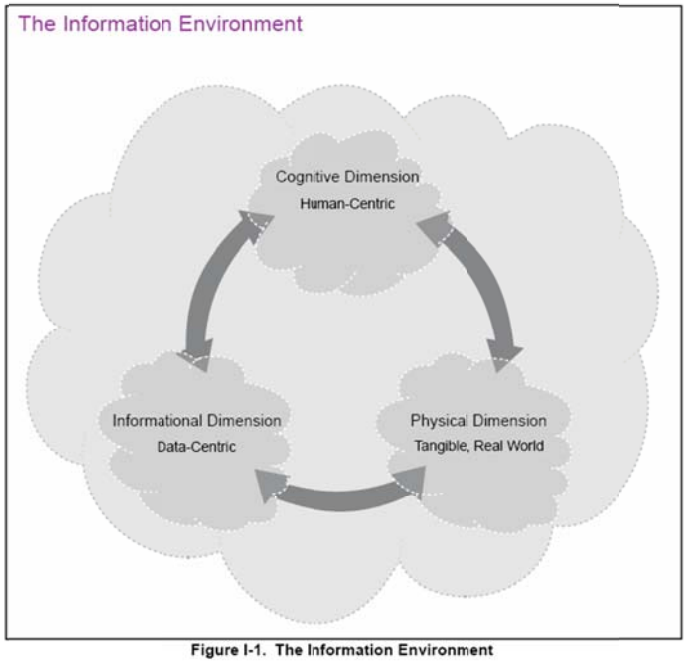


Figure I-1. The Information Environment

Figure 4

In comparing Figure 3 to Figure 4 it is immediately apparent that the root cause of much system insecurity, the Cognitive Dimension, is substantially absent from the Semantic eScience framework. JP 3-12(R), *Cyberspace Operations,* observes:

> [T]he strongest encryption and most secure protocols cannot protect our networks from poorly trained/motivated users who do not employ proper security practices.

There is little doubt that when Advanced Persistent Threat breach data are analyzed, the conclusions will almost always be that the attackers gained network privileges as the result of undesirable user behavior such as falling victim to spearphishing, engaging in poor password practices and vulnerabilities created through disregard of cybersecurity policies. A cyberattack is often an information operation designed to use people to gain and maintain system access. A crucial tool in this information operation is human deception, the subject of JP 3-13.4, *Military Deception*. Understanding successful adversary operations can often be gained by applying the Military Deception Maxims set forth in JP 3-13.4, *Military Deception.* **Deception is absent from Semantic eScience.**

Cybersecurity is highly dependent upon the user credential system, a system which exists outside of the Semantic eScience framework. For example, the problem that allowed criminals to access

sensitive taxpayer data on over 330,000 taxpayers from the IRS (http://krebsonsecurity.com/2015/08/irs-330k-taxpayers-hit-by-get-transcript-scam/) and permits criminals to fraudulently enter deaths into the U.S. Electronic Death Registration System (EDRS) (http://www.computerworld.com/article/2966130/cybercrime-hacking/def-con-how-to-virtually-kill-someone-or-cash-in-on-fake-babies.html) is excessive reliance on poorly conceived knowledge-based authentication (KBA) schemes, not malware or internal system errors. The interaction between users and systems, summarized graphically in Figure 5, is set forth in JP 3-12(R), *Cyberspace Operations*:

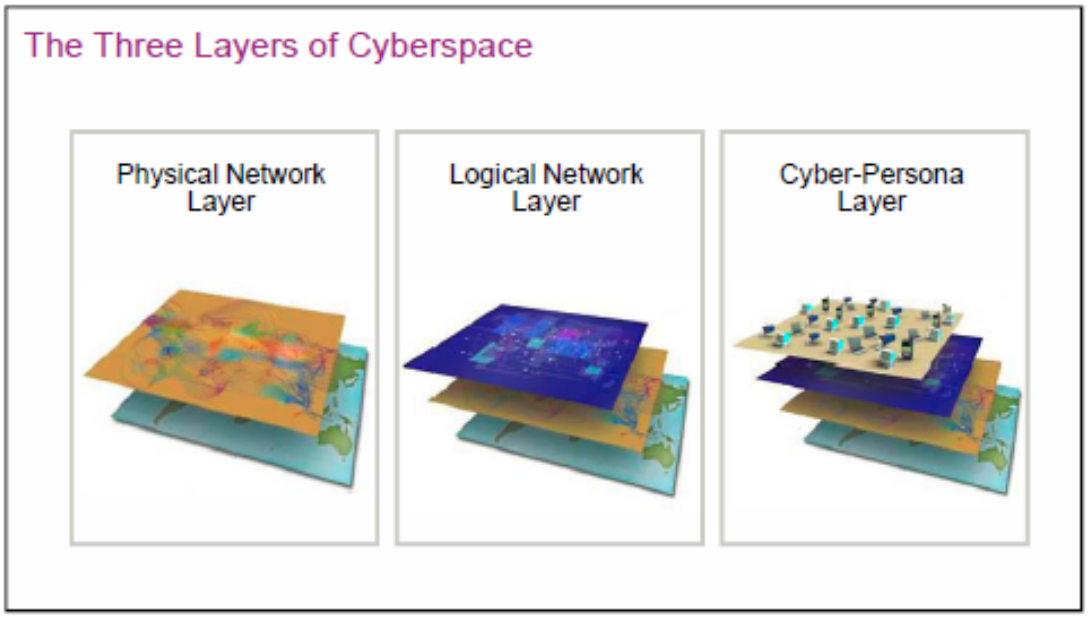


Figure I-1. The Three Layers of Cyberspace

Figure 5

Measurable Security. Measureable Security must be in the context of some objective. Joint Doctrine provides systems of assessment consistent with the topic of the respective publication.

Risk. Assigning numerical values to unknowable future events has been termed "Scientism" by Taleb and Martin in *How to Prevent Other Financial Crisis*, http://www.fooledbyrandomness.com/sais.pdf. Moreover, focusing on technical issues as the primary system vulnerability turns a blind eye to the easily exploitable user attack surface in which deception is used to obtain real credentials. See, for example, CERT Insider Threat Center. *Unintentional Insider Threats: A Review of Phishing and Malware Incidents by Economic Sector* (CMU/SEI-2014-TN-007). Software Engineering Institute, Carnegie Mellon University, 2014. P. ix, Web. 08 June 2015, http://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_297777.pdf. DHS Secretary Johnson summed it up more succinctly:

"What amazes me when I look into a lot of intrusions, including some really big ones by multiple different types of actors, it often starts with the most basic active spear-phishing where somebody is allowed in the gate and penetrates a network simply because an employee clicked on something he or she shouldn't have."

The concepts of risk and the communication of risk are pervasive in Joint Doctrine.

Agility. The idea that automated systems can provide rapid response is belied by experience. Automated systems are nothing more than a compilation of rules which defend against previously observed attacks. Successful attacks evade automated defenses because attackers respond to the actions of defenders by changing the attack attributes in response to defensive actions. This is discussed in detail in Rand's *The Defender's Dilemma: Charting a Course Toward Cybersecurity*.

There is nothing cyber specific about attackers changing in response to defenders. This general human interaction is termed “The Paradox of Warning” in JP 2-0, *Joint Intelligence*. The Paradox of Warning is a human engagement which, looking at the Information Environment of JP 3-13, *Information Operations*, is driven in the Cognitive Dimension by the decisions of attackers, users and analysts.

Human Factors. While the role of people is critical in cybersecurity, this use of the term “Human Factors” is a misnomer for two reasons. First, the term “Human Factors” describes a well-established field of psychology which is different than the proposal of this theme. Under the Sematic eScience proposal, the term “Human Factors” will mean one thing in the Science of Security and something else in the rest of science, such as when NIST, the federal agency responsible for promulgating guidance and regulations under FISMA and other areas of human health, safety and performance uses the term “Human Factors.” Second, the role of people in cybersecurity is far richer than merely “operational measurements of the human(s) running the operations.” A better concept for this theme is provided by JP 3-13, *Information Operations*; that concept is the Cognitive Dimension. Human beings are an important security exposure that merit far more attention than making operational measurements. In fact, as JP 3-13, *Information Operations,* observes, **[the cognitive] dimension constitutes the most important component of the information environment**.

Conclusion

Semantic eScience provides a constricted vision, losing sight of the operational environment that exists outside of its narrow purview.

Joint Doctrine provides the principles required for the Science of Security cyber ecosystem. Semantic eScience is a valuable tool for data analysts to apply within the Joint Doctrine framework. The Science of Security should adopt the Joint Doctrine framework and implement Semantic eScience as a tool for analysts within that framework.