The increasing number of cyber attacks on military networks and servers has raised the question of what the global defense community is doing to safeguard military systems and protect the larger global Internet.

Ubiquity's editor interviewed Chris Gunderson, who served in the U.S. Navy from 1973 to 2004 and became an expert in "network centric" warfare, on this question and in particular on how military philosophy must change to adapt to the rise of information networks.

Gunderson makes several references to Admiral Arthur Cebrowski, whom Ubiquity staff interviewed in August 2004 (see www.acm.org/ubiquity/interviews/v5i24_cebrowski.html).

Peter Denning
Editor

Are Militaries Lagging Their Non-State Enemies in use of Internet?

An Interview with Chris Gunderson

by Peter Denning

Chris Gunderson (chris.gunderson@w2cog.com) is on the Naval Postgraduate School faculty. The Joint Interoperability Test Command sponsors him to develop and improve "GIGlite." GIGlite, an activity of W2COG, links distributed government and industry laboratories to create an e-portal of government certified "net-ready" software products and services. Gunderson retired as a Captain after 27 years as a U.S. Navy Military Oceanographer. He was decorated for his service as the commanding officer of two large Navy Oceanography organizations and as the Deputy Oceanographer of the Navy. He is the founder of the Worldwide Consortium for the Grid.

Ubiquity: *How long have you been a student of military strategy?*

Gunderson: Since 1973, when I went to the U.S. Naval Academy. After graduating, I spent 27 years in uniform immersed in military thinking, and retired as a Captain. I became an advocate of "network centric" military strategy after reading Vice Admiral Art Cebrowski's U.S. Naval Institute Proceedings groundbreaking article on "Network Centric Warfare" in 1998.

Ubiquity: *What is different about military strategy today as compared with a generation ago, or with the earlier parts of the previous century?*

Gunderson: In early days nations were relatively quick to go to war with each other. As weapons evolved and armies grew, the cost of war on all participants became

increasingly steep. Hence, nations increasingly tended to avoid wars unless absolutely necessary, and the principle of "winning hearts and minds" became increasingly prominent in military thinking.

When war is necessary, opinion has been divided between "total war" and limited "surgical" wars. The emergence of nuclear deterrence as a strategy in the Cold War added many nuanced dimensions to the arguments. Since the Cold War, numerous "non-state actors"—mostly terrorist and quasi-military groups—have entered the arena and have been the strategic targets of state-supported militaries.

Some experts such as Tom Barnett, who was mentored by Admiral Cebrowski, now advocate developing a new kind of military that wins hearts and minds as a pre-emptive strategy against non-state actors.

Ubiquity: *Why has prevention become as important as conflict?*

Gunderson: Until fairly recently, nation-states often used military force to achieve national or religious objectives, such as gaining wealth or souls. Cost of wars waged for those ends were high, but calculable and recoverable.

The modern emergence of nuclear weapons changed everything by making the cost of total war untenable. Non-state aggressors have found it to be an effective strategy to hide in and among a sympathetic population, rendering traditional military tactics against them untenable. All these factors push the military center of gravity toward prevention of conflict.

Ubiquity: *Who was Art Cebrowski?*

Gunderson: Art Cebrowski (1942-2005) was a heroic Naval aviator who understood these trends and advocated that the military should critically reexamine itself and question the status quo. He earned quite a reputation for rocking the boat and at the same time earned wide respect for his unconventional views and analyses. For example, he believed that the Navy's beloved strategy of organizing around a relatively few large, powerful platforms—ships, carriers, and aircraft—should give way to relatively many small, fast, and agile platforms.

One of his biggest ideas was achieving tactical advantage through "information superiority"—the use of sensors, networks, and decision-assisting machines to achieve a decisive advantage. He developed the theory of network centric operations and warfare around that idea.

In 2001, the U.S. Secretary of Defense appointed him as the director of a new "Office of Force Transformation" to lead the defense department in that direction. He and everyone else realized that moving the military to network centric operations was not just a matter of developing and fielding the right technology, it was a social transformation—the winning of hearts and minds of military people.

Ubiquity: *What are the principles of his framework?*

Gunderson: Cebrowski suggested at least four big ideas:

1) connect military platforms, weapons, sensors, and information sources via modern routable computer networks,

2) co-evolve military processes with rapidly evolving IT analogously to sway the best commercial companies do that. In other words, keep up with Moore's Law,

3) design for the delivery of relevant, timely, and accurate information,

4) disparate units should *self-synchronize*, a term he coined, according to their shared understanding of their *commanders' intent*.

Ubiquity: *What was driving Cebrowski's concern? Why not just ride the tide along with everyone else adopting the Internet?*

Gunderson: Cebrowski believed that these four principles would achieve information superiority, an asymmetric information advantage over enemies. He believed that the U.S. Military had asymmetric advantage in all other areas of technology and war-fighting, an advantage that served as a powerful deterrent to war. But the rise of free, open, and ubiquitous information technology and networks was leveling the playing field and destabilizing global security by giving non-state actors a place to hide. He believed that these principles were the means to achieving superiority in the information domain as well as the others.

Ubiquity: *Has anyone implemented those principles?*

Gunderson: Cebrowski's ideas were considered radical. They challenged cherished beliefs about chains of command, delegation of authority, and use of open systems. It is very impressive that the defense community—and not just the U.S. Department of Defense, pretty much the entire international defense community—has embraced his principles. It is taking time to put them into practice.

I personally am a loyal and passionately supportive member of that global defense community, and have been for 36 years. That said, I'm going to be deliberately provocative in my reply.

On the surface, it would seem that Cebrowski's four netcentric principles are a natural fit to the military. They are completely supportive of well-understood principles of successful teamwork: communicate, innovate, empower, and collaborate. The military is exquisitely good at training its members to be excellent at teamwork and coordination. Their lives and their missions depend on it.

However, the military sees Internet technologies as an evolutionary addition to its traditional suite of specialized communications equipment. We in the military have an almost paranoid concern for security of communications—just look at what happened to the Germans in WWII when the British cracked their impregnable Enigma cipher with Alan Turing's machine at Bletchley Park. The concern for communication security leads in the opposite direction from the open Internet.

Despite more than a decade of policy documents supportive of netcentric principles and operations, the concern for security has trumped the netcentric policies in actual practice. That is, despite spending billions of dollars with the expressed purpose of fielding network centric capability, the defense community has generally not succeeded at implementing distributed netcentric systems. Rather, we cling to the notion that military communications requirements are unique. We make "sunk cost arguments" about the value of our specialized legacy networks.

On the other hand, many terrorist groups, such as Al Qaeda, and criminal groups, such as the Mexican Drug Cartels, have applied the netcentric principles to achieve information superiority via the open Internet and World Wide Web. I find it alarming that enemies are gaining an asymmetric advantage over us using technology we invented.

Ubiquity: *What is this "sunk cost" idea?*

Gunderson: It's the notion that once you have invested an enormous sum in a way of doing business, you can't change it because you would lose all the money you've sunk into the investment that far. Even though it is clear that the old way is not succeeding any more, you continue because of inertia. This notion affects the military thinking because of the tremendous investment in proprietary communication technologies. It just doesn't seem right or sound to abandon those concepts, investments and technologies.

Ubiquity: *Are you saying that the U.S. Military should give up its private networks?*

Gunderson: Essentially, yes. More precisely, I believe we in the global defense community should give up using private networks for the great bulk of our communications. If you want to fight and win a war, you have to be master of the terrain. In the information war "the terrain" is the Internet and the World Wide Web.

In the past "military communications" were indeed a very specialized capability. When public communications were wired telephones, telegraphs, and letters then it made perfect sense for militaries to develop and maintain capability like signal flags, tactical links, and encrypted CW radios. But now the U.S. Military is like the frog in the pot who hasn't noticed that the water's now boiling. Adversaries now have better communications and related technology than allies. Our traditional military partners are mostly in the same boat, or rather, the same boiling pot.

Consider transportation networks as an analogy. Some specialized military vehicles, such as tanks, cruisers, and fighter jets, need additional armor and weapons. However, military vehicles generally use the same highways, air routes, and sea-lanes as commercial vehicles. Militaries do not build their own road systems, they invest their limited resources to augment the existing transportation network in ways necessary to perform their specialized missions, for example, tactical bridges, mine hunting, close air support, strategic underwater patrols.

Ubiquity: *Aren't communication technologies more critical than roads? Isn't abandoning propriety communication systems except for specialized needs far too radical to ever be implemented?*

Gunderson: Maybe, but individual soldiers and sailors have always found ways to innovate in the grey areas outside the bounds of official policies. Certainly, in my career my colleagues and I have found ways to "augment" the official tool kit with trips to Radio Shack. I hear from friends that folks in battle zones today are using commercial-off-the-shelf (COTS) technologies in innovative and unofficial ways. I'm simply suggesting that we should take this productive innovative activity—activity that authorities have always winked at—out of the shadows.

Ubiquity: *Allowing soldiers to innovate isn't quite the same thing as eliminating military reliance on private networks.*

Gunderson: I honestly don't see the value added by the military's private unclassified Intranet. In fact, I think our special military "dot mil" URL provides a "bulls eye" for hackers to aim at. Further, the majority of the traffic on military classified networks is not classified or even particularly sensitive. I really believe U.S. and coalition forces would be better served if we issued them cell phones, trained them that "loose lips sink ships," and gave them open access to the Web. In the limited situations when warriors need to use classified networks, they should exercise old fashioned "circuit discipline"—no idle chatter or spamming.

Did you know that in response to a recent cyber breach the U.S. defense community has outlawed thumb drives from its networks? These portable drives had been just as ubiquitously useful for military applications as they are for civilian purposes. By forbidding their use, we have essentially executed a denial of service attack on ourselves!

If I were the U.S. Secretary of Defense I would mandate using the open Web as the principal military communication domain. However, I would also invest heavily in the research and engineering required to make the Internet more secure, and in particular to provide highly secure channels through the open Internet.

Ubiquity: *What sort of investments do you have in mind?*

Gunderson: We need security services that do a better job protecting secrets than PayPal does protecting credit cards. We need traffic routing services that are less vulnerable than Domain Name Servers (DNS.) We need ubiquitous computer network defense capabilities that aggressively "sniff" and respond to malignant cyber activity.

Ubiquity: *Why has it been difficult to implement those principles?*

Gunderson: National governments tend to be deliberative and cautious. Those tendencies manifest themselves in layers of bureaucracy. Government acquisition processes are no different. "Acquisition" process is the set of methods and procedures for acquiring new systems and new technologies. Over the years, in the U.S., the Congress and leaders of the acquisition bureaucracy have accreted many restrictions designed to limit fraud and reduce risk of failure in the systems delivered.

We must abide by laws requiring us to separate funding for basic research, engineering, and operations, to meet workforce distribution requirements, to avoid illegal export of information, and to eschew government-industry collaboration in the name of avoiding "conflict of interest." These controls have been effective at mitigating some of the issues, such as fraud, they were designed to alleviate.

The downside of all these restrictions is that the time for the government to procure and deliver a major system is easily a decade or more. With the environment of use changing at the rate of Moore's Law, the delivered systems are almost always obsolete or obsolescent.

Ubiquity: *So the time constant for delivery far exceeds the time constant for the world to change?*

Gunderson: Exactly. The Worldwide Consortium for the Grid, or W2COG, is an open innovation forum I founded for the U.S. Defense Department in 2004 to help advance the development of military networks. W2COG members recently ran an experiment to compare the traditional acquisition process with an open development process.

After 18 months, the team following the traditional process had spent $1.3 million and produced a concept paper. The open development team produced a working prototype with 80 percent of the desired functionality in three months for $300,000. The traditional process is simply not capable of keeping up with the rapidly changing world.

Ubiquity: *What other factors impede adoption of open Internet in the military?*

Gunderson: Military Services, agencies, and organizations compete aggressively with each other for resources in the defense arena. They all wind up with independent, incompatible information systems and information practices. It is very hard to join all these large, expensive systems into a coherent global defense network.

These are just a few examples of many factors that create an environment anathematic to Cebrowski's principles. It is virtually impossible to acquire a new system in less than a decade. It is impossible to keep up with Moore's Law in information technology with the current acquisition system. Everything delivered is near obsolete by the time of delivery. Even if we could overcome the fear of compromise of communication security, we would not be able to field the needed systems in time for them to be useful in military operations.

Ubiquity: *Don't governments have fast-track methods of acquiring systems?*

Gunderson: They do. Certainly in the U.S. defense community we have various rapid prototyping and "COTS insertion" initiatives. Indeed, these programs have been very successful in many ways. For example, as far as I know we fielded all the coalition tactical Unmanned Aerial Vehicles (UAV)—obviously very successful inventions—through fast track methods. However, these fast track initiatives tend not to have mechanisms to sustain the capability beyond the life of the initially deployed items. In my opinion, the success of these fast track projects proves the value of much of what Cebrowski advocated for the acquisition process—and if we could learn to do this as a regular practice rather than a fast-track exception, we would be able to sustain information superiority.

Ubiquity: *Let's go back to the W2COG, the World Wide Consortium for the Grid. What is that all about?*

Gunderson: W2COG is an example of U.S. Defense Department leaders addressing the dilemma we discussed above. Einstein said, "You can't solve a problem with the same thinking that created it." The defense community processes are not "bad" they just were not designed to address the threats and environment we find ourselves in today.

Recognizing that reality, senior leaders in U.S. Department of Defense chartered the U.S. Naval Post Graduate School to create the not-for-profit W2COG. We sought to adapt the highly successful process in the W3C (World Wide Web Consortium) to the development of military networks. W2COG uses "best practices" from Internet social networking and "e-biz" models to create an alternative process and "dot org" environment for distributed, focused, collaborative engineering among government, industry, and academic experts.

Ubiquity: *What have you learned about how to fix the acquisition processes since starting W2COG?*

Gunderson: I've learned that the best way to achieve powerfully disruptive change is by subtly co-opting the existing processes. By "co-opt" I don't mean anything subversive or underhanded. I simply mean we should introduce more convenient and efficient methods within the constraints of the existing bureaucratic requirements. The improvements will be adopted because they are perceived as both comfortable and useful. For example, acquisition policy requires program managers to perform "analysis

of alternatives," or AoA, prior to making design decisions. Typically, AoA takes the form of long, expensive paper studies. The W2COG alternative is quick consultation with an independent panel of experts followed by rapid demonstration of working code to appropriate certification authorities. The W2COG way is faster, better, cheaper and... legal under the policy.

I've also learned that the most critical technical issues that we must overcome, in addition to the security issues we already discussed, is how to alleviate information overload.

Ubiquity: *Information overload? Is that a problem in the military?*

Gunderson: Absolutely, and it is often life threatening. Alvin Toffler was one of the first to use the term "information overload" to describe situations where the vast quantities of data overwhelmed the brain's ability to process it effectively. As a result a person cannot make well-grounded decisions. In developing the Network Centric Warfare concept, Cebrowski and his colleagues John Gartska, Dave Alberts, and Fred Stein, went to great lengths to draw analogies to traditional military theory. "Fog and Friction of War" is a classic metaphor meaning that warfare is always messy and unpredictable. We might consider information overload as the "fog" of network centric war.

Ubiquity: *What can we do to eliminate "information fog?"*

Gunderson: I once talked to Admiral Cebrowski about this. At the time, senior military officers mistakenly believed that Cebrowski claimed that computer networks could negate the fog and friction of war. They feared that network centric warfare (NCW) was all about allowing "arm chair quarterbacks in the Pentagon" to run battles from a distance. In that context, I asked Cebrowski how he felt Admiral Nelson's strategy and tactics at Trafalgar compared to the theory of NCW.

Nelson was famously skeptical of the new technology of the time, signal flags. Advocates believed that by using signal flags, admirals could negate fog and friction of war and execute perfect control of their fleet throughout the battle. Nelson's alternative approach was to invest hours and hours of his time in continuous personal dialog with his ship captains. He taught them his ideas. He listened to their ideas. They discussed strategies and tactics endlessly. They also practiced pre-arranged strategies and tactics using signal flags. Nelson did not use the flags to control action, but rather to enable effective independent operations.

When it was time to fight the battle, all Admiral Nelson had to do was to signal his general intentions. His captains needed no additional signals. Lacking computer networks, they relied on a "network" of mutual trust and individual innovation to mass their strength against enemy weakness, that is, achieve asymmetric advantage. Cebrowski concluded that Admiral Nelson was, in fact, an expert practitioner of NCW. Cebrowski himself called this the doctrine of "commander's intent" and practiced it himself in all his commands. He believed that the network technology was not what

conferred an advantage, but the skillful practices of coordination and ability to adapt to local conditions by taking local actions consistent with the commander's intent.

So my answer is that we can give the good guys better "visibility" in the fog of information overload in two ways.

First, we can train our network of information providers in practices that send critical information and avoid bogging down warriors with large volumes of data. Critical information is any information that would cause someone to change tactics in pursuit of the commander's intent. For example, a pilot follows a flight plan (the commander's intent) unless the sensor network reports a thunderstorm to deviate around; most of the time the sensor network reports nothing because there is no need to change the flight plan.

Second, and most importantly, we can empower and teach our warriors to be as independently innovative as Admiral Nelson's Captains. Nelson taught them to take action in the face of uncertainty, watch the consequences, and quickly adapt if things start to go wrong.

Ubiquity: *What's your prognosis?*

Gunderson: I'm optimistic! In my work with the W2COG, I see a growing center of mass of frustrated experts "in the trenches" of the acquisition process. They are starting to view vague netcentric acquisition policy directives as "commanders' intent" rather than as an excuse for inertia. They are beginning to "self synchronize" around some disruptive new approaches.
I think there will soon be a number of low profile netcentric engineering success cases. As the new processes prove their value, larger programs will gradually adopt them as a matter of course. The frog and his allies will again find themselves thriving in a nice cool pond... catching flies at will.