White Paper
Representing the NCOIC Advisory Council Views

The August 2012 NCOIC joint Advisory Council Board of Directors meeting provided direction that the NCOIC should elevate its studies and processes to include analysis of policies and procedures along with technology that ensures and or prevent interoperability capability.

The Dec 2012 NCOIC joint Advisory Council Board of Directors meeting delved further into this subject. The council discussions provided a format by which the NCOIC could test the process that expanded the philosophy from technical interoperability to policies and processes that assist and prevent interoperability. The council believed that the cyber security arena has profound needs but has a minimal business value because of the existing policies procedures.

The council discussed the need for a system similar in concept to fire codes, which are processes, procedures, best practices and standards to guide the evolution of policy and rules. A similar issue is now within the FAA and they have been working on standards and procedures to control and protect the flow of information at all aspects of the air transport system. The NCOIC should consider those actions and determine how it could be applied to other areas.

The FAA representative concurred, and mentioned a new concern; unmanned aircraft. FAA does not have all the answers but they are continuing to work on cyber security.

Several members indicated they have watched both the US congress and the NATO countries struggle with cyber legislation and to date they have not passed any laws dealing with cyber security. Within the US there is pending a draft Presidential Executive Order on how to deal with critical infrastructure, and it tasks the NIST to develop a cyber framework that ties to international standards. The intent is to avoid the US just looking to US standards. The Executive Order asks about incentives to help advance the cause of cyber security, for example, giving an advantage to vendors who bid on government business if they comply with the NIST standards. Directives are fine to a point however there needs to be a business case or business model that incentivizes companies to create a common cyber defense. This model needs to be international in concept.

Shifting to the concept from directives to incentives the NCOIC team that will do the study should consider these types of incentives along with the cyber code standards.

At the low end of managing cyber risk for the masses of individual users, standards can be a big help and industry best practices are constantly being applied here...there are many readily available commercial tools. However, at the high end/high risk/critical infrastructure arena, cyber protection is based on talent and processes that can be brought to bear quickly. Therefore the study should start with the high end issues.
The NATO representatives highlighted the NATO experience in Afghanistan. The weakest link in the chain of 28 member nations plus the additional coalition partners makes all and the entire system vulnerable. There is a need for commonality of protection. This was identified in the Afghan Mission Network analysis and lessons identified. NATO intends to address cyber requirements across the Alliance and for the Future Mission Network. The idea of a common set of cyber “fire codes” could be very helpful. If the NCOIC can come up with some concepts that enable cross system cyber security it would be of great benefit.

The advisory council chair summarized the discussion. The council recommended that the NCOIC develop a discovery process that will identify top level technologies and then identify the policies and procedures that inhibit cross domain use. The end result is that the team should provide some policy or procedural concepts that would incentivize businesses to create a strong cyber environment.
Attachment A: Presidential Executive Order

THE WHITE HOUSE
Office of the Press Secretary

EMBARGOED UNTIL DELIVERY OF THE PRESIDENT'S STATE OF THE UNION ADDRESS
February 12, 2013

EXECUTIVE ORDER

- - - - -

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation’s critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

Sec. 2. Critical Infrastructure. As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters.

Sec. 3. Policy Coordination. Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive-1 of February 13, 2008 (Organization of the National Security Council System), or any successor.

Sec. 4. Cybersecurity Information Sharing. (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the “Secretary”), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of
section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

(c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with 6 U.S.C. 143 and in collaboration with the Secretary of Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13569 of August 19, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.

(e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

Sec. 5. Privacy and Civil Liberties Protections. (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency’s activities.

(b) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security (DHS) shall assess the privacy and civil liberties
risks of the functions and programs undertaken by DHS as called for in this order and shall recommend to the Secretary ways to minimize or mitigate such risks, in a publicly available report, to be released within 1 year of the date of this order. Senior agency privacy and civil liberties officials for other agencies engaged in activities under this order shall conduct assessments of their agency activities and provide those assessments to DHS for consideration and inclusion in the report. The report shall be reviewed on an annual basis and revised as necessary. The report may contain a classified annex if necessary. Assessments shall include evaluation of activities against the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles, and frameworks. Agencies shall consider the assessments and recommendations of the report in implementing privacy and civil liberties protections for agency activities.

(c) In producing the report required under subsection (b) of this section, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of DHS shall consult with the Privacy and Civil Liberties Oversight Board and coordinate with the Office of Management and Budget (OMB).

(d) Information submitted voluntarily in accordance with 6 U.S.C. 133 by private entities under this order shall be protected from disclosure to the fullest extent permitted by law.

Sec. 6. Consultative Process. The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. As part of the consultative process, the Secretary shall engage and consider the advice, on matters set forth in this order, of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies; other relevant agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts.

Sec. 7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure. (a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), and OMB Circular A-119, as revised.

(b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures
and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

(d) In developing the Cybersecurity Framework, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, the National Security Agency, Sector-Specific Agencies and other interested agencies including OMB, owners and operators of critical infrastructure, and other stakeholders through the consultative process established in section 6 of this order. The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information and technical expertise to inform the development of the Cybersecurity Framework. The Secretary shall provide performance goals for the Cybersecurity Framework informed by work under section 9 of this order.

(e) Within 240 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework (the "preliminary Framework"). Within 1 year of the date of this order, and after coordination with the Secretary to ensure suitability under section 8 of this order, the Director shall publish a final version of the Cybersecurity Framework (the "final Framework").

(f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, experience from the implementation of section 8 of this order, and any other relevant factors.

Sec. 8. Voluntary Critical Infrastructure Cybersecurity Program. (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the "Program").
(b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

(c) Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.

(d) The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.

(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.

Sec. 9. Identification of Critical Infrastructure at Greatest Risk. (a) Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established in section 6 of this order and draw upon the expertise of Sector-Specific Agencies. The Secretary shall apply consistent, objective criteria in identifying such critical infrastructure. The Secretary shall not identify any commercial information technology products or consumer information technology services under this section. The Secretary shall review and update the list of identified critical infrastructure under this section on an annual basis, and provide such list to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs.

(b) Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section. The Secretary shall develop a process for other relevant
stakeholders to submit information to assist in making the identifications required in subsection (a) of this section.

(c) The Secretary, in coordination with Sector-Specific Agencies, shall confidentially notify owners and operators of critical infrastructure identified under subsection (a) of this section that they have been so identified, and ensure identified owners and operators are provided the basis for the determination. The Secretary shall establish a process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications under subsection (a) of this section.

Sec. 10. Adoption of Framework. (a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, these agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director of OMB, and the Assistant to the President for Economic Affairs, that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.

(b) If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13609 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.

(c) Within 2 years after publication of the final Framework, consistent with Executive Order 13563 and Executive Order 13610 of May 10, 2012 (Identifying and Reducing Regulatory Burdens), agencies identified in subsection (a) of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.

(d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are
encouraged to engage in a consultative process with the Secretary, relevant Sector-Specific Agencies, and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

Sec. 11. Definitions. (a) "Agency" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) "Critical Infrastructure Partnership Advisory Council" means the council established by DHS under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments.

(c) "Fair Information Practice Principles" means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(d) "Independent regulatory agency" has the meaning given the term in 44 U.S.C. 3502(5).

(e) "Sector Coordinating Council" means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor.

(f) "Sector-Specific Agency" has the meaning given the term in Presidential Policy Directive-21 of February 12, 2013 (Critical Infrastructure Security and Resilience), or any successor.

Sec. 12. General Provisions. (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.

(d) This order shall be implemented consistent with U.S. international obligations.

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at
law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA

THE WHITE HOUSE,
February 12, 2013.

# # #
In Cyberwar, Software Flaws Are A Hot Commodity

Tom Gjelten February 12, 2013

There have been security flaws in software as long as there has been software, but they have become even more critically important in the context of cyberweapons development.

In the past, security researchers who stumbled on a software flaw would typically report the flaw to the manufacturer of the software, so it could be fixed. That changed, however, when cyberweapon designers started looking at these flaws as vulnerabilities that could serve as a back door into a computer network. Most prized of all were "zero day vulnerabilities" - flaws whose existence was previously unknown.

Richard Bejtlich was a cyber specialist for the U.S. Air Force in the 1990s, a time when the U.S. military was going on the offense in the cyberwar. He remembers the day he realized how important a software vulnerability can be to a cyberweapons designer.

"Myself and a couple other guys, we found a zero day vulnerability in Cisco routing equipment," Bejtlich recalls. "And we looked at it, and we said, 'Did we really find this? Can we really get into these Cisco routers?'"

They could, and so Bejtlich and his colleagues reported it to Cisco. The company thanked him and said it would be fixed. Days later, he was talking to some friends who worked on the offensive side of the unit, and they had quite a different reaction to them reporting the bug to Cisco.

"They said, 'You did what? Why didn't you tell us? We could have used this to get into all these various hard targets,' " he says.

To Bejtlich, a software flaw was simply a mistake to be corrected. To a cyberweapons designer, however, it was a potential back door into the computer network he wanted to attack.

"We actually had a standing order after that," Bejtlich says, "that said, if you find something, you don't tell the vendor, you tell the offensive side, and they'll decide what to do about it."

Potential Dangers

A potential loser here, at least in the short run, is the consumer who may be stuck with a flawed piece of software because the government doesn't want anyone to know about the flaw, seeing it as something that could be exploited for the deployment of a cyberweapon.

ACLU technologist Christopher Soghoian, who is something of a privacy activist, says this is something people should know about.

"I don't think your average small business, medium-sized business or Fortune 500 company realizes what's going on here," Soghoian says. "I don't think they realize that their government knows about flaws that could be fixed, and
is sitting on them and exploiting them against other people rather than having them fixed."

A good example would be the Stuxnet worm, used by the U.S. and Israel to attack computers controlling nuclear operations in Iran. The designers of Stuxnet took advantage of a software bug in the Microsoft Windows operating system, without alerting Microsoft to the flaw.

The demand for software vulnerabilities has grown to such an extent that the researchers who discover them no longer need to settle for a software vendor sending them a thank-you note, or even a small cash reward. In the context of escalating interest in cyberwar, there is now a growing global demand for the software vulnerabilities - the back doors - that allow an attacker to get inside his enemy's computer network.

"For every researcher who's doing the right thing [by alerting the vendor] and getting the modest gift," Soghoian says, "there are plenty of researchers who are selling these things for what they deem to be the true market value.

"And the true market value is whatever governments and their middlemen are willing to pay."

'It's Just Business'

Former Airman Bejtlich, now the chief security officer at Mandiant, a cybersecurity firm, is not in the business of selling vulnerabilities to the highest bidder, but he knows other cyber people who are.

"There seems to have been an explosion of interest in the last maybe two years," Bejtlich says, "where the hot thing to do is to found a company with five of your buddies who are all really good at finding vulnerabilities and just start making money."

Given that this interest is spurred by the development of secret cyberweapons research, the vulnerability market by necessity operates mostly in the shadows. When the vulnerability traders make a public appearance, it's usually at a conference where hackers and other cyber researchers gather to discuss their latest work.

A vulnerability seller named Donato Ferrante showed up recently at the "Suits and Spooks" conference in Arlington, Va. In an interview with NPR, Ferrante said he advertises his vulnerabilities through an email list. His clients see what vulnerabilities he has found in which products, but Donato gives only the barest of information about the flaws.

"If the customer wants [to] use the vulnerability, the customer needs to buy the vulnerability," Ferrante said. "This is just a sort of portfolio; then the customer needs to buy the details."

Ferrante's company, ReVuln, is the seller. For them, "it's business," he says.

An Unregulated Market

In the U.S., the National Security Agency and other branches of the U.S. military, law enforcement and intelligence agencies are among the biggest
buyers of vulnerabilities. But there are other buyers, including any party with an interest in being able to penetrate an adversary’s computer network.

Besides the U.S., other governments are also developing cyberweapons. Some private companies may have an interest in penetrating a rival company’s network. For that matter, criminal organizations might be interested in purchasing vulnerabilities, or even groups plotting a cyberterrorist attack.

Not surprisingly, vulnerability sellers don’t want to say much about their business. Asked where he is based, Ferrante simply says, “Europe,” though in a subsequent email he clarifies that he operates out of Malta. He is not eager to describe the world in which he works.

“I don’t see bad guys or good guys,” Ferrante says. “It’s just business.”

After all, Ferrante says, Revuln is only selling information. “The way the information is used is up to the customer; it’s not up to us.”

There is no regulation of the vulnerability market in the U.S. There is a law prohibiting the export of software that provides penetration capabilities that would enable the users to attack, deny, disrupt or otherwise impair the use of computer infrastructure or networks. But there is no mandatory reporting of vulnerability sales.

If the sellers are not aware of the use to which their vulnerabilities will be put, they may not be prosecutable.

“I am shocked that this has not been regulated,” Bejtlich says. “It would be so easy for a legislator to say, ‘We’re going to do arms control. We’re going to keep this out of the hands of the bad guys. You’re going to need a license to have these tools.’"

“Who’s going to stand up and say, ‘No, you have to have cyberweapons!’ I mean, if you wanted to look for an easy way to have legislators appear to be doing something, this would be it,” he says.

The vulnerability trade is just one example of many that indicates how developments in cyberwarfare, and the development of cyberweaponry, are proceeding so quickly that the thinking about how to manage this new domain of warfare is not keeping pace.

Transcript

RENEE MONTAGNE, HOST:

Wars have long been fought on land, on sea and in the air. Now there’s a new battlefield — cyberspace. Countries, the United States included, are launching attacks on each other’s computer networks. Software can be a lethal weapon. This week, NPR’s Tom Gjelten is looking at the offensive side of cyber war. Today, the cyber arms market — how computer weapons are developed, bought and sold around the world.

TOM GJELEN, BYLINE: To understand how a cyber-attack works, think of it like a burglary. First, you have to get inside the place you’re going to burglarize. You do that by picking a lock or maybe you can sneak in through a back door someone left open. Only then, when you’re inside, can you carry out the
crime. Technologist Christopher Soghoian says it’s the same thing when you attack a computer network.

CHRISTOPHER SOGHOIAN: You need a way of getting in the door. You need a way of getting into the system that you’re hacking into, whether it’s the computer of a surveillance target or the computer running a nuclear power plant. So you need a way in.

GJELTEN: Once you’ve found that way in, once you’ve penetrated a network, you instruct the computer to do what you want. But these are separate operations, and Soghoian says the first step in a cyber-attack is often the most challenging.

SOGHOIAN: The code that you run that steals data, that taps the microphone, this is easy stuff to write. The code that gets in the door is really sophisticated, very difficult and completely unregulated.

GJELTEN: Here’s the trick. All computer systems linked to the Internet use applications like Internet Explorer or Adobe. These programs inevitably have bugs in them. Some are security flaws. They’re like that back door someone neglected to lock. Cyber researchers call these bugs vulnerabilities because they expose the program to intruders just as an open window makes a house vulnerable to burglary.

When security researchers found these bugs in the past, they’d report them to the software manufacturer so they could be patched. But then the cyber weapon designers came along and set their sights on the vulnerabilities. They’d actually call them back doors because they could serve as back doors into a network.

They didn’t want to patch them. They wanted to exploit them. The weapon designers especially liked the vulnerabilities nobody else knew about. In cyberspeak these are called zero days or O-days. Richard Bejtlich, a former cyber specialist in the Air Force, remembers the time back in the ’90s when he first realized a software vulnerability was something a cyber weapon designer could exploit.

RICHARD BEJTLICH: Myself and a couple other guys, we found a zero day vulnerability in Cisco routing equipment, and we looked at it and we said, did we really find this? We can really get into these Cisco routers? Yes, we can. So what did we do? Called up Cisco, told them, hey, we found this vulnerability, and they go, thank you for telling us, we’ll work on fixing it.

A couple days later, I’m talking to some of my friends who work on the offensive side of the unit and I said, yeah, we actually reported this O-day to Cisco. And they said, you did what? Why didn’t you tell us? We could have used this to get into all these various hard targets.

GJELTEN: To Bejtlich, a software flaw was a mistake to be corrected. But that was the view from the defensive side. Air Force guys assigned to offensive cyber operations saw that software flaw as an open door into the network they were trying to attack.

BEJTLICH: We actually had a standing order past that point that said if you find something, you don’t tell the vendor, you need to tell the offensive side, and then they’ll decide what to do about it.
GJELTEN: What this means is that if the military thinks a software flaw can be used for a cyber weapon, it may not want anyone else to know about it. Christopher Soghoian with the Speech Privacy and Technology Project at the ACLU says consumers, individuals and businesses could be the losers here.

SOGHOIAN: I don’t think they realize that their government knows about flaws that could be fixed and is sitting on them and exploiting them against other people rather than having them fixed.

GJELTEN: That’s just one issue. There’s more. The greater interest there is in a capability to launch cyber attacks, the more demand there is for those software vulnerabilities, the back doors that allow an attacker to sneak into someone’s network. There’s now a global market for back doors. Soghoian says private researchers who discover a software flaw have a choice - alert the manufacturer and maybe get a little reward or share that vulnerability with a potential cyber-attacker for a big payoff.

SOGHOIAN: For every researcher who’s doing the right thing and getting, you know, the modest gift, there are plenty of researchers who are selling these things for what they deem to be the true market value. And the true market value is whatever governments and their middlemen are willing to pay.

GJELTEN: Former Air Force officer Richard Bejtlich is on the private side himself now, as chief security officer at Mandiant, a cyber consultancy. He’s not in the business of selling vulnerabilities to the highest bidder, but he knows other people who are.

BEJTLLICH: There seems to have been an explosion of interest in the last maybe two years, where the hot thing to do is to found a company with five of your buddies who are all really good at finding vulnerabilities and just start making money.

GJELTEN: Essentially we’re talking here about a cyber arms market. Not surprisingly, it operates mostly in the shadows, but at conference last weekend I caught up with one seller of back door vulnerabilities. His name is Donato Ferrante. He says he advertises his vulnerabilities through an email list. Clients see what back doors he has found into which software products, but they get only the barest information about the vulnerability.

DONATO FERRANTE: If the customer wants to use the vulnerability, the customer needs to buy the vulnerability. This is just a sort of, you know, portfolio and then the customer needs to buy the details.

GJELTEN: And would you sell them?

FERRANTE: I mean if they want to buy, yeah. I mean this is our job. It’s business.

GJELTEN: It’s business. Between the U.S. military, law enforcement and intelligence agencies, the U.S. government is a big buyer of vulnerabilities or back doors. But it’s not only the U.S. developing cyber weapons. So are other governments. Private companies wanting to penetrate an adversary’s network may also be in the market for back doors. So could cyber criminals, for that matter, or even groups plotting a cyberterrorist attack.
No wonder vulnerability sellers don't want to say much about their business. Donato Ferrante says he's based in Europe, but won't say which country. I want to know more.

What's this world like that you work in?

FERRANTE: It's just, you know, I don't see, you know, bad guys or good guys. It's just business.

GJELTEN: No bad guys or good guys, just clients. After all, Ferrante says, he's just selling information.

FERRANTE: The way the information, you know, would be used, it's up to the customer. It's not, you know, up to us.

GJELTEN: At the moment, there is virtually no regulation of the back door market in the United States, no mandatory reporting of vulnerability sales, for example. Richard Bejtlich of Mandiant.

BEJTLICH: I am shocked that this has not been regulated, because to me it would be so easy for a legislator to say, we're going to do arms control. We're going to keep this out of the hands of the bad guys. You're going to need a license to have these tools. And who's going to stand up and say, no, you have to have cyber weapons.

I mean, if you wanted to look for an easy way to have legislators appear to be doing something, this would be it.

GJELTEN: But developments in cyber warfare and cyber weaponry are moving so fast that our thinking about this new domain of combat and crime just can't keep pace. And it's not just governments finding new ways to attack each other. Private firms frustrated by their inability to defend their networks against cyber-attacks are increasingly going on the offense themselves. That story tomorrow.

Tom Gjelten, NPR News. Transcript provided by NPR, Copyright NPR.

Copyright 2012 National Public Radio (Source).