Schneier on Security

Computer Network Exploitation vs. Computer Network Attack

Back when we first started getting reports of the Chinese breaking into U.S. computer networks for espionage purposes, we described it in some very strong language. We called the Chinese actions cyber-attacks. We sometimes even invoked the word cyberwar, and declared that a cyber-attack was an act of war.

When Edward Snowden revealed that the NSA has been doing exactly the same thing as the Chinese to computer networks around the world, we used much more moderate language to describe U.S. actions: words like espionage, or intelligence gathering, or spying. We stressed that it's a peacetime activity, and that everyone does it.

The reality is somewhere in the middle, and the problem is that our intuitions are based on history.

Electronic espionage is different today than it was in the pre-Internet days of the Cold War. Eavesdropping isn't passive anymore. It's not the electronic equivalent of sitting close to someone and overhearing a conversation. It's not passively monitoring a communications circuit. It's more likely to involve actively breaking into an adversary's computer network -- be it Chinese, Brazilian, or Belgian -- and installing malicious software designed to take over that network.

In other words, it's hacking. Cyber-espionage is a form of cyber-attack. It's an offensive action. It violates the sovereignty of another country, and we're doing it with far too little consideration of its diplomatic and geopolitical costs.

The abbreviation-happy U.S. military has two related terms for what it does in cyberspace. CNE stands for "computer network exploitation." That's spying. CNA stands for "computer network attack." That includes actions designed to destroy or otherwise incapacitate enemy networks. That's -- among other things -- sabotage.

CNE and CNA are not solely in the purview of the U.S.; everyone does it. We know that other countries are building their offensive cyberwar capabilities. We have discovered sophisticated surveillance networks from other countries with names like GhostNet, Red October, The Mask. We don't know who was behind them -- these networks are very difficult to trace back to their source -- but we suspect China, Russia, and Spain, respectively. We recently learned of a hacking tool called RCS that's used by 21 governments: Azerbaijan, Colombia, Egypt, Ethiopia, Hungary, Italy, Kazakhstan, Korea, Malaysia, Mexico, Morocco, Nigeria, Oman, Panama, Poland, Saudi Arabia, Sudan, Thailand, Turkey, UAE, and Uzbekistan.

When the Chinese company Huawei tried to sell networking equipment to the U.S., the government considered that equipment a "national security threat," rightly fearing that those switches were backdoored to allow the Chinese government both to eavesdrop and attack US networks. Now we know that the NSA is doing the exact same thing to American-made equipment sold in China, as well as to those very same Huawei switches.

The problem is that, from the point of view of the object of an attack, CNE and CNA look the same as each other, except for the end result. Today's surveillance systems involve breaking into the computers and installing malware, just as cybercriminals do when they want your money. And just like Stuxnet: the U.S./Israeli cyberweapon that disabled the Natanz nuclear facility in Iran in 2010.

This is what Microsoft's General Counsel Brad Smith meant when he said: "Indeed, government snooping potentially now constitutes an 'advanced persistent threat,' alongside sophisticated malware and cyber attacks."

When the Chinese penetrate U.S. computer networks, which they do with alarming regularity, we don't really know what they're doing. Are they modifying our hardware and software to just eavesdrop, or are they leaving :logic bombs" that could be triggered to do real damage at some future time? It can be impossible to tell. As a 2011 EU cybersecurity policy document stated (page 7):

> ...technically speaking, CNA requires CNE to be effective. In other words, what may be preparations for cyberwarfare can well be cyberespionage initially or simply be disguised as such.

We can't tell the intentions of the Chinese, and they can't tell ours, either.

Much of the current debate in the U.S. is over what the NSA should be allowed to do, and whether limiting the NSA somehow empowers other governments. That's the wrong debate. We don't get to choose between a world where the NSA spies and one where the Chinese spy. Our choice is between a world where our information infrastructure is vulnerable to all attackers or secure for all users.

As long as cyber-espionage equals cyber-attack, we would be much safer if we focused the NSA's efforts on securing the Internet from these attacks. True, we wouldn't get the same level of access to information flows around the world. But we would be protecting the world's information flows -- including our own -- from both eavesdropping and more damaging attacks. We would be protecting our information flows from governments, nonstate actors, and criminals. We would be making the world safer.

Offensive military operations in cyberspace, be they CNE or CNA, should be the purview of the military. In the U.S., that's CyberCommand. Such operations should be recognized as offensive military actions, and should be approved at the highest levels of the executive branch, and be subject to the same international law standards that govern acts of war in the offline world.

If we're going to attack another country's electronic infrastructure, we should treat it like any other attack on a foreign country. It's no longer just espionage, it's a cyber-attack.

This essay previously appeared on TheAtlantic.com.

Tags: backdoors, cyberespionage, cyberwar, espionage, essays, hacking, national security policy

Posted on March 10, 2014 at 6:46 AM • 22 Comments

Comments

Bob S. • March 10, 2014 7:23 AM

As usual Bruce you are right, "It's no longer just espionage, it's a cyber-attack."

One problem, with rare exception, is American leaders in a position to do anything about it are stone silent. That includes the President, Congress and Supreme Court among others.

Also, the big picture is, though millions of people are alarmed by our country's militancy and corrupt conduct, there are just as many or more millions who support it or simply don't care.

Meanwhile, the military-corporate lobby is well disciplined, organized and aggressive.

The only hope is enough people get mad as hell and simply won't take it anymore.

I see the odds as slim.

not everyone is spying or hacking • March 10, 2014 7:32 AM

Bruce - please stop saying "everyone is doing it" - it isn't true. Only a few very advanced countries are actually playing seriously. Everyone _can_ play and when _everyone_ is actually playing, we're going to see serious consequences.

Please please stop spreading the lie that "everyone is spying" or "everyone is hacking" - this is a bias and it reflects on your perception of who is included in "everyone."

Almost no one is even able to spy on the entire planet - that is why we must secure the planet before *other* nations have similar capabilities.

doof • March 10, 2014 7:41 AM

Bruce,

Do you draw a line between a curious or troublemaking kid and a military use of CNE? I fear that efforts to consider all forms of CNE to be acts of war will further push efforts against hacking to be the next war of drugs.

AlanS • March 10, 2014 8:01 AM

@Bruce

The disturbing difference is not the breaking-in versus passive listening part but the surveillance being baked into the technical infrastructure. Under CALEA this a legal requirement in the US.

Clive Robinson • March 10, 2014 8:08 AM

With regards the language please remember,

> One man's freedom fighter is another man's terrorist

The language differential is the same it's all spin used for FUD, just as "think of the children" are used to distort peoples perception.

With regards CNE and CNA they are by most juresdictions --of interest-- legislated crimes with significant penalties. The fact that it is done by other nations under the "National Security" excuse does not make it any less a crime nor does "tit for tat" / "eye for an eye" reasoning make it not a crime on the supposed excuse of "self defence".

I would prefer we did not call it "Cyber-warfare" for similar reasons to not calling certain questionable actvities "economic-warfare" because the lend a "legitamacy" to criminal activities that they don't deserve and it also makes follow on crimes in retaliation appear as "legitimate defence" it's not.

Warfare in all it's forms are barbaric acts that states try to legitamize under "rules of war" which are more apparent in their breach than in their observance. The first Gulf war had some small legitamacy but the subsiquent "War on Terror" and it's following activities are not legitimate acording to international treaty that the wester beligerants have signed up to. And no mater how many weasle minded lawyers paid and dependent on the state declair otherwise by trying to change the meanings of words so far they are not just twisted but totaly unrecognisable, those acts make the wester beligerants guilty of war crimes.

As was once observed "Fair words, do not, of a pigs ear make a fine silk purse".

Benni • March 10, 2014 8:41 AM

The problem with this is:
Things like stuxnet then could never be deployed. As the US is not in war with iran, it could not make cyper attacks on iran, if cyber attacks can only be done under the law of war.

In the distant future, it may nevertheless turn out that these things will be military operations.

By more and more complex attacks, aginst everybody the attacked states (which are all nations) will eventually figure it out that cyber attacks are operations that are part of war.

But i fear that will take some time. It similarly took time, until a law of war was made.

Saul Tannenbaum • March 10, 2014 8:55 AM

There is, of course, nothing new about this.

Consider the days of the Cold War when the US and the Soviet Union used agents under "non official cover" to perform a range of actions against each other.

Espionage? Preparation for war?

Both.

What made this sustainable was a set of gentlemen's rules along with the realization that it was in neither sides' best interests to let things escalate out of control because at the end of that chain of escalation was nuclear war.

It's an interesting question whether we can find a similar set of understandings when the agents of infiltration are binary rather than human.

---

name.withheld.for.obvious.reasons • March 10, 2014 9:35 AM

In Bruce's blog post about the use of computing to perform surveillancethat the find/fix/finish (code name WATERWITCH)issue DEFINES the new cyber warfare battlespace and the impacts on real lives.

This is exactly what is defined in PPD 20, the use of kinetic force in combination with cyber warfare.

This makes cyber warfare and the associate lexicons more than just talk/code.

We have to get past these models of InfoSEC, EMSEC, cyber warfare, and other ontology that does little to but put a label on an object/concept--descriptions that can make real the issue and affect the necessary changes are what's needed--today.

Chris.S • March 10, 2014 10:01 AM

First you state:

> But we would be protecting the world's information flows -- including our own -- from both eavesdropping and more damaging attacks. We would be protecting our information flows from governments, nonstate actors, and criminals.

Then you immediate state:

> We would be making the world safer.

Could you please elaborate on how the second follows from the first? I can see that it is certainly **sometimes true**, but I can also see cases where I'm fairly certain it is **not true**.

---

vas pup • March 10, 2014 10:58 AM

@Bruce:"In other words, it's hacking. Cyber-espionage is a form of cyber-attack. It's an offensive action. It violates the sovereignty of another country, and we're doing it with far too little consideration of its diplomatic and geopolitical costs." Intelligence of 21 century due to new technologies of collecting information could not be mainly restricted to Humint and Osint. Intelligence including penetration like CNE without planting time bombs or other destructive (actual or delayed) activity to the network or target tied to it are not cyber-attack in the sense which required retaliation within cyber space only or by kinetic force as well. If you change in previous sentence 'without' to 'with', then it it cyber attack as you suggested. Now, Intelligence is break down not only by means, but by the nature (target) of collected information. That is why exist CIA and DIA, not just one Agency. Set of targets of cyber-espionage may escalate CNE to CNA even without (see above) based on nature of the targets (military secrets related to actual defense capabilities, locations/operation procedures/etc. of strategic military /defense /offence objects) because their place on the top of National Security and in the core of its infrastructure. That area is not yet clearly defined and required very cautious steps moving forward to develop the whole framework of cyber war with final step as International Convention like with WMDs. But it order to work, as the first step, it should be accepted the idea that International Law is equally applied to and respected by all parties involved. That is my point.

Skeptical • March 10, 2014 12:32 PM

I think Chris S. asks the big question with respect to overall information security policy above.

I also think we should be very, very careful about categorizing actions undertaken regularly by advanced states (CNE) as acts of war. Do we really want the US Government to consider it an act of war to attempt to penetrate its computer systems? Do we want anyone else to consider such attempts to be acts of war?

Currently US policy on the matter is that cyber operations against it may incur a proportional response in any domain that the US chooses. So, a nation conducts espionage. The US catches them. It would not be proportional to declare war on the nation conducting espionage.

By contrast, a nation plants a logic bomb that results in the explosion of a power plant. Now that's something that would trigger a military response, and not necessarily in the cyber domain.

That policy makes sense to me. But I don't understand a one-size-fits-all, if it's CNE then it's war, policy. What are the advantages of it? Unless CNE presents such a grave threat that we must deter it by threatening war against any nation that undertakes such operations, it seems unwise to unilaterally declare such operations to be acts of war.

Shawn Smith • March 10, 2014 1:59 PM

Skeptical asked on March 10, 2014 12:32 PM

> What are the advantages of it?

I'm going to put on a cynical hat here and say that it allows military and government contractors to make lots and lots of money, especially for the people at the top of the organization chart. And since those are the only people who really matter, that is reason enough.

65535 • March 10, 2014 2:17 PM

"…Offensive military operations in cyberspace, be they CNE or CNA, should be…recognized as offensive military actions, and should be approved at the highest levels of the executive branch, and be subject to the same international law standards that govern acts of war in the offline world." -Bruce S.

I agree. But, the lines are purposely blurred and are hidden via secret courts. The term "National Security" has been grossly bloated to include just about every level of attack and a catch word for "legal circumvention of the Fourth Amendment" and by extension an attack on the First Amendment. By twisting words for the sake of "National Security" laws become meaningless.

Once you start down the path of weaponizing all electronic communications you cause an arms race. The by-product of this arms race will certainly spread far and wide and will trickle down to cyber criminals – and maybe trickle-up from cyber criminals to other actors.

It becomes cyber free-for-all fight which includes a vast array of players from nation states to criminals to political and economic actors bent on power and wealth. The end result could damage American companies, American jobs and sow suspicion and distrust in the global market place for years to come.

Brandioch Conner • March 10, 2014 8:18 PM

> *In other words, it's hacking. Cyber-espionage is a form of cyber-attack. It's an offensive action. It violates the sovereignty of another country, and we're doing it with far too little consideration of its diplomatic and geopolitical costs.*

Bruce, espionage has ALWAYS been an "attack" by that definition.
Rosenberg

Espionage is different from an "attack". You address espionage with your own espionage or through diplomatic channels. Claiming it is an "attack" is a problem.

---

mud man • March 10, 2014 8:38 PM

The problem is that, from the point of view of the object of an attack, CNE and CNA look the same as each other, except for the end result.

In the MAD old days, worry about somebody covertly obtaining a first-strike capability was a big destabilizer. I wonder how much that obtains here? Oh, I forgot, we don't do that cold war shit any more.

Figureitout • March 10, 2014 10:22 PM

Brandioch Conner
--It very much is an attack. The meaning of the word in the days of the Rosenberg's has changed to how trivially easy it can be to get way too much info on you. Did credit cards exist back then? Was encryption

(shitty broken old systems at that) common place then? I can sit in my house and get all the neighbors router MAC addresses trivially easy w/ pentesting software that is freely given out on the internet. And once you acquire enough info, now essentially you can launch attacks for the rest of the victim's life unless s/he purges and takes some extreme evasive actions...

It's really sick, and it's hard to focus on meaningful things w/ so much crude everywhere and forced to use the internet to survive. Just today found another interesting malware (or stupid malfunction) on my school computers that puts an "invisible" box on your screen but task manager makes it disappear...Ending process "dwm.exe" at least made it visible. And now my school is pushing my disk space online to google instead of hosting a local storage space.

---

bemused • March 10, 2014 10:31 PM

@Brandioch: to say nothing of the fact that the the "we" Bruce cites in order to argue for an equivalency between cyber espionage and attack comprise three distinct groups: Google, journalists, government. It is google and journalists who are using the word "attack" rhetorically to dramatize espionage activities of the Chinese; it is the government who argues that espionage activities are a peacetime activity not warranting a military response.

Fundamentally, you argue that gathering intelligence should by itself be construed as an act of war. This is clearly absurd. Taking a picture of a sensitive facility could be done to learn about whats going on there, or to blow it up, or all of the above- war will happen when facility is blown up, not when the picture is taken. With CNA your network/server goes down; with CNE it doesn't: how do those states in any way resemble each other? That CNE is a precondition for CNA (in many cases) hardly implies an equivalency between the two.

Autolykos • March 11, 2014 5:19 AM

"We can't tell the intentions of the Chinese, and they can't tell ours, either." - And there is no rational reason you should trust each other anyway, because you got a serious commitment problem right there. Even the best treaty signed in the most noble and honest intentions (by both sides) wouldn't be worth the paper it's printed on.
Once you start hacking their computers, there is no point in limiting your capabilities, since going whole hog doesn't cost anything extra or even increase risk of detection.

FP • March 11, 2014 9:20 AM

Re: "Much of the current debate in the U.S. is over what the NSA should be allowed to do."

From my point of view, it's more limited. Most of the current debate is over what the NSA should be allowed to do to *Americans*.

Most Americans don't seem to have a problem with what the NSA is doing to other nations, and many are rather proud of the NSA capabilities. After all, the others are out to destroy the US, and we must be able to destroy them first!

Andrew • March 12, 2014 11:46 AM

@Bemused:"Fundamentally, you argue that gathering intelligence should by itself be construed as an act of war. This is clearly absurd. Taking a picture of a sensitive facility could be done to learn about whats going on there, or to blow it up, or all of the above- war will happen when facility is blown up, not when the picture is taken. With CNA your network/server goes down; with CNE it doesn't: how do those states in any way resemble each other? That CNE is a precondition for CNA (in many cases) hardly implies an equivalency between the two."

We're not talking about taking pictures from outside the facility in regard to CNE, though. That sort of reconnaissance has its analogies in the digital realm by way of scanning & fingerprinting and, if you're lucky enough to have the visibility, watching who comes and goes *at the perimeter*. This requires no exploitation, apart from privileged presence between the visitors and the facility (telco or TAPs) for the last point.

This CNE discussion is about the attacker entering the facility by subverting or compromising the security mechanisms that prevent this unauthorized access - at Civilian installations to a large degree - unavoidably by means that also enable other adversaries. Bruce's points that I emphatically agree with are that 1.) our capabilities should be focused upon securing these security mechanisms, *including* for civilian installations, instead of systematically weakening controls required for the way our economy currently operates (see BULLRUN) and 2.) gaining unauthorized entry to a secured facility by compromising its security mechanisms is an attack. If an actor breaks through your perimeter and alters trusted assets (malware, implants) inside the facility they can justifiably be considered a hostile adversary.

Tell the "why care about CNE if there's no CNA" story to those opposed to Iran & N.Korea developing nuclear capabilities. Except CNE goes further in that it isn't just developing technology but subverting that of others.

Brandioch Conner • March 12, 2014 12:39 PM

@Andrew

> *This requires no exploitation, apart from privileged presence between the visitors and the facility (telco or TAPs) for the last point.*

If it is Team A then it is "privileged presence".

If it is Team B then it is "exploitation".

That sounds too much like "it's not X because X is what our enemies do and we do not do that".

> *2.) gaining unauthorized entry to a secured facility by compromising its security mechanisms is an attack.*

The problem is the usage of the word "attack".

1. A script-kiddie defacing a web site can be described as an "attack".

2. A cracker using an exploit to get control of a server can be described as an "attack".

3. A spy sending nuclear secrets to a foreign government can be described as an "attack".

4. An invading army can be described as an "attack".

They are not equivalent. But there are people who claim that the response should be the same. Which is why we need to use more exact terminology.

> *If an actor breaks through your perimeter and alters trusted assets (malware, implants) inside the facility they can justifiably be considered a hostile adversary.*

And an enemy commando squad would also be considered "a hostile adversary".

But they are not the same as Robert Morris.

Eric Blaise • September 25, 2015 4:02 PM

I am surprised I have never thought of that, or seen it that way. Essentially, when cyber attacks occur, the country that is accused refers to it as gathering information, while those on the receiving end rightfully call it an attack. We look down on other countries for doing it, but it is quite widespread. It is not shocking since there is very little security as you go up in the network scale. Wide area networks (WAN) are less secure than LANs, and Global networks (the internet) are less secure than WAN's. They get a foothold layer by layer, until they get get into the smaller networks.

Subscribe to comments on this entry

Leave a comment

Login

Name (required):

E-mail Address:

URL:

□ **Remember personal info?**

Fill in the blank: the name of this blog is Schneier on ___________ (required):

Comments:

Allowed HTML: <a href="URL"> • <em> <cite> <i> • <strong> <b> • <sub> <sup> • <ul> <ol> <li> • <blockquote> <pre>

Preview Submit

← Friday Squid Blogging: Being a Jumbo Squid

FIREWALK: NSA Exploit of the Day →

Schneier on Security is a personal website. Opinions expressed are not necessarily those of Resilient, an IBM Company.