State of the Union: Cyberthreat

Summary: *President Obama signed a cybersecurity executive order yesterday. Our own David Gewirtz, one of America's leading cybersecurity experts, explains why Mr. Obama didn't go far enough.*

By David Gewirtz for ZDNet Government | February 13, 2013 -- 13:46 GMT (05:46 PST)

Normally, shortly after the President delivers his Constitutionally-mandated State of the Union report (it's the report that's required, not the speech), I deconstruct the speech (http://www.zdnet.com/blog/government/10-things-and-4-outrages-techies-need-to-know-about-president-obamas-state-of-the-union-address/9930) and provide you with the points I think are important to consider.

Today is not a normal day. While the union is undergoing its usual economic and political stresses, with the sad addition of increased gun violence, what I consider the most important story got only a two-paragraph mention in President Obama's speech last night.

America is being attacked. Constantly (http://www.zdnet.com/14-global-cybersecurity-challenges-for-2013-7000009352/) . Unrelentingly. We are being attacked (http://www.zdnet.com/is-preemptive-cyberwarfare-good-national-security-policy-7000010857/) by enemy nation states (like North Korea), frenemy nation states (like China and Russia), friendly nation states (like France and Israel), hacker groups (like Anonymous), just plain ol' organized crime organizations out to make a buck (http://www.zdnet.com/understanding-cybercrime-video-seminar-7000010120/) , and individual hackers out to make a name for themselves.

Read this

Obama's cybersecurity executive order: What you need to know

Read more

Although the President only gave the cyberthreat two paragraphs of attention in his speech, he did something else very important yesterday: he issued an Executive Order, "Improving Critical Infrastructure Cybersecurity" (full text (http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity) , ZDNet analysis (http://www.zdnet.com/obamas-cybersecurity-executive-order-what-you-need-to-know-7000011221/)).
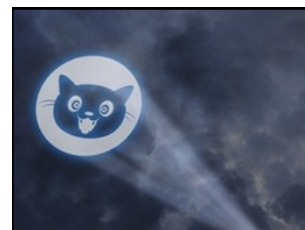
It is at this point that I must share with you an important disclosure about myself. I am a member of the FBI's InfraGard program, the infrastructure security partnership between the FBI and industry. I am also a member of the U.S. Naval Institute and the National Defense Industrial Association, the leading defense industry association promoting national security. I'm also the Cyberwarfare Advisor to the International Association of Counterterrorism and Security Professionals.

I'm telling you this because you need to know that I look at these issues from a similar perspective as those in Homeland Security and the other three-letter agencies. We have a challenge here: we are being attacked. We have a second challenge: we Americans cherish our privacy and any defense has to also protect that privacy.

Let me be blunt: I don't think President Obama went far enough.

Mr. Obama's Executive Order is a step in the right directly, but it's not strong enough and may even open the door to new exploits.

I also think President Obama missed a golden opportunity to involve the American people. In fact, I think he squandered a necessary, critical, golden opportunity – using the bully pulpit of the State of the Union and its worldwide media coverage to involve American citizens in their own cyberdefense.

On the other hand, the Executive Order generally gets the privacy protection side of things pretty much right. Previous attempts at cybersecurity legislation have forgotten the the importance of privacy. When CISPA and SOPA were spun up, so were the forces of We The Internet, and rightly so. Those were both bad law-making and they were rightfully squashed.

President Obama's new Executive Order takes those concerns into account. "Privacy" is mentioned 14 times in the order. Section 5 of the document is entitled, "Privacy and Civil Liberties Protections," and provides substantial and reasonably guidelines for the ongoing maintenance of our sacred freedoms.

This is supported by a statement from the ACLU (quoting from an article (http://thehill.com/blogs/hillicon-valley/technology/282699-obama-signs-cybersecurity-executive-order-) in The Hill):

"The president's executive order rightly focuses on cybersecurity solutions that don't negatively impact civil liberties," Michelle Richardson, a legislative counsel for the ACLU, in a statement. "For example, greasing the wheels of information sharing from the government to the private sector is a privacy-neutral way to distribute critical cyber information."

Unfortunately, in its first run through Congress, CISPA seemed to miss the point (http://www.zdnet.com/privacy-killer-cispa-is-coming-back-whether-you-like-it-or-not-7000011056/) about America freedom and privacy. I am not convinced that additional legislation, especially the way CISPA was written, is necessary to protect America, since our existing laws about crime, espionage, and warfare pretty much cover the defensive aspects of the cyberthreat.

I am also deeply concerned about reports (http://www.techdirt.com/articles/20130212/02540821948/despite-protests-congress-to-bring-back-cispa-exactly-as-it-was-last-year-while-obama-signs-exec-order.shtml) that CISPA is back on the table, essentially unchanged. Sadly, in 5 reasons why SOPA, PROTECT-IP and other legislative idiocy will never die (http://www.zdnet.com/blog/government/5-reasons-why-sopa-protect-ip-and-other-legislative-idiocy-will-never-die/11087) , I predicted this sort of thing would keep on happening.

On the other hand, the new Executive Order seeks to set mandatory cybersecurity standards for government agencies and voluntary standards for U.S. companies and organizations.

However, as malware guru Phil Owens mentioned to me in yesterday's cybersecurity webcast (http://www.techrepublic.com/webcasts/live-webcast-title-14-cloud-security-challenges-for-2013/32765765) , once you set standards, you also set a minimum bar for acceptability. Essentially, you're telling agencies and businesses that "this is good enough," and you're telling attackers, "This is what we're watching for," leaving the door open for attack vectors not covered in regulations.

My ZDNet colleague and friend Zack Whittaker points out (http://www.zdnet.com/obamas-cybersecurity-executive-order-what-you-need-to-know-7000011221/) that the terms "cyberthreat" and "cyberintrusions," remain relatively undefined. His contention is that those "hacktivist" organizations that choose to use Distributed Denial of Service (DDoS) attacks as a form of protest speech (http://www.zdnet.com/privacy-killer-cispa-is-coming-back-whether-you-like-it-or-not-7000011056/) might then be targeted by the US government.

My take on DDoS as protest speech is quite simple: DDoS is an attack that must be defended, and the attackers must be brought to justice. In fact, a DDoS attack is an asymmetrical attack, which means that the attackers often have a vast logistical advantage over the defenders.

There is a difference between a flash mob (or even a Million-Man March) and a DDoS attack. A DDoS attack uses computers infiltrated against the will of their users, and turns ordinary computer users into cannon fodder. It would be as if – when a group decided they wanted to conduct a flash mob in protest – they broke into millions of homes, kidnapped the residents, and dragged them along, just to raise their numbers for the TV cameras.

As someone who's had to defend against an attack from millions of computers a day aimed at a few private servers, I have not a shred of patience for anyone conducting a DDoS. There is no excuse for a DDoS and it is not and never will be a legitimate form of protest.

Moving on, I mentioned earlier that President Obama squandered a golden opportunity.

When the President discussed cybersecurity in his speech, he made it sound like something that's the concern of government and industry. Although he mentioned identity theft, he didn't involve the American people – moms, dads, grandparents, kids, teachers, students, office workers, Facebookers – in the discussion.

He didn't make the threat *real* to real Americans.

In World War II, when the Nazis were bombing London, the British government communicated the threat to their people. It was obvious, as bombs were dropping. But the government made it clear that *everyone* had some responsibility in the national defense.

They instituted blackout rules, requiring lights to be doused at night, or black curtains to be hung over windows. The reasoning was very practical. If a *Luftwaffe* bomber could see a lit building, it could hit the building.

Now, say there was an apartment building with 100 apartments. If even one resident ignored the blackout rules, the building might be hit, and hundreds of tenants might be killed – just because one person disregarded the defensive rules.

This is quite analogous to our cybersecurity problems today. We are not just getting attacked at the entry point to banking networks or federal agencies. No. In fact, most of the attacks are being conducted against regular American citizens, you, me, your mom, my dad, and so on.

If any one of us has poor defenses, malware (like the kind that tunneled into the New York Times last week) could make it into our home networks, and then spread from family member to family member, from home computer to work computer, from work computer to work network, and so on.

Where President Obama missed his opportunity was making this point. We, as Americans, will never *ever* have a comprehensive cybersecurity defense until every computer-using American is safe from attack. And every computer-using American won't be safe from attack until each of us fully understands both the risks and the methods of protection.

We need this to be a national priority, a message of Presidential import, and Mr. Obama missed it.

Until every American is on board, until every American is aware of the threat, until every American is actively involved in his or her own defensive behavior, cyberattackers have an easy, wide-open invitation to enter, pillage, and plunder our networks.

This is war. It's a war where, whether we like it or not, we're all combatants. I just wish President Obama had explained that to his fellow Americans.

Topics: *Security, Government, Privacy*

About David Gewirtz

David Gewirtz, Distinguished Lecturer at CBS Interactive, is an author, U.S. policy advisor, and computer scientist. He is featured in The History Channel special The President's Book of Secrets.

Related Stories
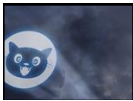
Obama's cybersecurity executive order: What you need to know
ZDNet

Obama signs cybersecurity executive order ahead of State Of The Union
ZDNet

How Do I Get My Credit Card Company to Settle My Bill for Less Than the Payoff Amount?
eHow.com

How to Read Your Credit Score - Edmunds Auto Finance Tips
edmunds.com

How to Read Your Credit Score - Edmunds Auto Finance Tips

Talkback

We need protection Obama
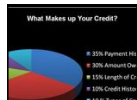
Rights are disappearing and made up rights are being created left and right.
Hoards of people that just exist for voting purposes have swung elections out of control.
It's disgusting how people are being treated like livestock, fed foodstamps, obamacare, endless
unemployment checks, etc and then brought to market to vote.

Representaion without taxation is killing this country.

eversso2
13 February, 2013 14:31

Reply   8 Votes

Gawd....

You have Internet access -- so what is your excuse to posting such inane, goofball drivel? The dog
ate your brain?

JustCallMeBC
13 February, 2013 15:06

Reply   6 Votes

It's probably the incest

Keeping it in the family has it's genetic and cognitive tolls...

T1Oracle
13 February, 2013 16:39

Reply   2 Votes

Disengage brain. Spout Fox News rhetoric.

Welcome to fear-induced cognitive manipulation by special interest media. Your brain has been
thoroughly washed of any independent thinking.

Reactionary morons are what is really killing this country. They ignore reality, morality,
compassion, the Constitution, and human rights. They move us closer to totalitarianism with
every "patriotic" decision they make. They react to every media sensation out of fear rather than

careful thought. They address symptoms rather than causes. More baseball bats and kitchen knives kill people each year than guns, yet we need to be disarmed. The mentally ill are the ones doing the mass killing, yet we aren't addressing mental health at all. Instead, we're attacking LEGAL gun owners. The criminals will ALWAYS have guns. Disarming the populace is meant to protect the government, not the people. They want to make law abiding citizens the helpless victims of anyone with a gun.

Here's another example: There are far more jobs available right now than there are people who are unemployed, yet these reactionary morons want to cut education funding which could enable unemployed people to fill those jobs and support themselves. People with little or no education are the ones filling most of our prisons. A large number of people turn to crime because they don't have the education to support themselves any other way. Many have a better life in prison than on the outside. Morons think helping the impoverished is expensive, when it's more than twice as expensive to feed, clothe, and house the same people in prisons. I remember seeing the taxpayer cost per prisoner and thinking the majority of those people would stop committing crimes if they made HALF that amount working. It would make more sense to train prisoners to do bridge and road construction, then hire them when they get out to repair our crumbling infrastructure instead of housing them indefinitely. If we included free job training as part of our poverty programs, the number of poor would decrease substantially over time, and more people would be in the middle class.

This would benefit the government because the middle class are the only ones paying full tax rates. The poor don't make enough to be taxed and the very rich have bought enough Congressmen to create the loopholes they need to avoid paying their fair share. The rich are the only ones enjoying "representation without taxation." Their influence upon our government is a trillion times higher than any poor person. Any person the poor help elect is immediately turned into a puppet by the rich upon arrival in Washington.

Morons make decisions based on artificial media-induced fear. Intelligent people see the actual causes of the problems and address those, rather than what media is telling them to address. In other words, they think for themselves rather than parroting the sound bites special interest owned media broadcast. Try it sometime.

BillDem
13 February, 2013 18:39

Reply   *2 Votes*

More Education?

K12 is free, but they fail to graduate huge numbers of kids, and graduating K12 you basiaclly need an 8th grade education.

Anyone with a pulse can get into college to "get their learn on" and load of with federal loans.

Most fail college classes and never graduate.

Gee money well spent.

Three things fix about everything:
1. Flat tax 10-20%, no credits, no deduction for corps or personal AT ALL.
2. Prisions are all now work camps, all cost paid for by some product or service by prisoners.
3. Allow success and ALLOW failure. Right now succes is punished and failure rewarded.

eversso2
13 February, 2013 19:02

Reply   Vote

What Rock Did You Crawl From Under?

Voting is a RIGHT granted by the U.S. Constitution. Treated like livestock? No more people are being treated like humans, because of these programs. I must, also, point out that many people that think like you have thought that some people should not vote. Some will defend, "with their lives", the right to own a gun, but the right to vote--well that is just not that important. About swinging out of control: "The People" have swung control of the vote in their favor, contrary to your thinking. No, they didn't go the way you think they should, but, again, you are only a majority of one!! Peace!

eargasm
13 February, 2013 17:07

Reply   2 Votes

This revolutionary war happened

because of taxation without representation, why then is representation without taxation ok?

Last year 51% of country paid nothing in income taxes, up from 47%.

It's probably even worse for 2012 nearly climbing near 60%, the number should be ZERO.

eversso2
13 February, 2013 17:16

Reply   2 Votes

I'll ask the question again

Where are you getting these stats?

John L. Ries
13 February, 2013 19:44

Reply   *1 Vote*

He can't tell you

as he make them up or his friends, the nutcase part of NRA that have taken over, has told him so. And if it is like any other with his opinions, accepted without asking for source of the data. Because if asked, it could turn out being false.

Jxn
15 February, 2013 16:15

Reply   *Vote*

Voting is a right?

All the U.S. Constitution originally did was to make the qualifications for voting for members of the House of Representatives (originally the only directly elected federal institution) the same as for the "most numerous branch" of the state legislature, effectively allowing each state to make its own rules). We've passed a number of amendments since then that have prohibited various forms of discrimination, but to this day, it's the states that at least theoretically determine the qualifications for voting.

Of course, that has nothing to do with "rights", which are not legal entitlements, but moral ones.

John L. Ries
13 February, 2013 19:44

Reply   *Vote*

Proof

http://www.youtube.com/watch?v=tpAOwJvTOio

everss02
13 February, 2013 17:26

Reply   *Vote*

There is a balancing act at work here

The dopey SOPA/PIPA/CISPA garbage freaked out a lot of people over excessive government snooping and loss of privacy and liberty, so Obama had to carefully tread a middle ground here.

JustCallMeBC
13 February, 2013 15:12

Reply   3 Votes

There's a flaw in the WWII analogy...

People living in London were living in perfectly normal houses. These were designed to have windows which let light out. They weren't designed to deter bombing raids and in fact, those happened VERY rarely when you look at London as a city that's been around for almost 2000 years in one form or another.

The internet, on the other hand, is new, has been changing continuously and, as you note, is always under attack. (Sidenote - everyone everywhere is always under attack in the internet - at least in part because everyone defines 'attack' differently. So framing this as an 'American' problem is kind of superficial.)

The solution isn't to build bunkers - it's to fix the internet.

The internet got started within a very closed group (DARPA and then educational institutions) where obscurity by isolation made per-user security unimportant. Then the net leaked out to the real world and that shortsightedness has plagued us ever since.

Something as simple as base level packet encryption on ALL packets would have helped. A mail protocol that wasn't wide open and had *some* kind of authentication requirements would have helped. An IP addressing scheme that had enough addresses to handle at least the actual population of the world would have been smart because then NAP would never have existed, as would an IP address registration system equivalent to the global DNS system - but also acting as an address *invalidator* (so unassigned addresses could safely be rejected) and so on.

The state of "cybersecurity" to day is the result of many bad decisions made over the years by the architects and caretakers of the internet. Time to stop blaming the people who just use the net and start blaming the people who botched (and are still botching) the design of it.

TheWerewolf
13 February, 2013 16:51

Reply   2 Votes

Good points

But until we do, we need to make sure people are safe. We also need to fix our bridges and bring back Firefly and Buffy, but I don't see those happening, either.

David Gewirtz

Reply   Vote

Agreement with david and thewerewolf

I agree with david on the point that americans should need to be trained in the area of cyberwarfare. Relatively few americans are without a PC (excluding the amish and other very violence neutral people). Training in cyberwarfare is good similar to handing an american an gun though (very bad people would prefer to use it for bad purposes). But similar to being taught proper handling of a knive in royal rangers or boyscouts. if someone gets a special license or takes a class to own a gun then some unstable people would not get a gun because they would not pass any tests (Similar to a drivers license in the fact that you can buy from anyone you choose as long as you have a license.). Knowledge is the first step but offering cybersecurity classes to people at community centers would be a tremendous help effort in the area of the United States I live in. As I have been learning david in my security class malware that exploits "social engineeing" tactics is most prevelant in the wild so it would require giving knowledge to us citizens about at the minimum common procedure.
Also, I agree with the werewolf in the fact that poor standards or poor updates to the current computing standards leave lots of room for improvement. your issue david is more one of documentation and trying to do too complicated encryption and authication procedures that no-one knows how they can be improved. For example, the flaw found in WEP encrpytion for wireless networks involved authentication issues but WPA does not have those issues (I will try to remember where in my book i found that and I think their was a magazine article or scholarly article too on this).

jeffman_z

Reply   1 Vote

No i was not talking about licensing computers.

Sorry, I hope I did not confuse people about licensing guns as an Analogy to licensing computers that is not what i meant but training citizens on proactive approaches is good thinking.

jeffman_z

Reply   Vote

Joe Sixpack ain't a cybersecurity expert.

But he figured out he could go on down to Walmart and buy one of them durn 'puters and plug it in. Nobody bothered to tell him he could instantly become a victim and unintended accessory to cybercrime. That 'puter just sits there getting slower and slower, he doesn't know why, and it's part of a botnet attacking a bank or defense contractor or sending spam out to people like him.

Back when it was only enthusiasts who had computers, there wasn't such a problem because enthusiasts tend to keep up with the technical details instead of just how to get on the facebook and play the angry birds games.

I can't say much more about it without coming off as some sort of elitist who does nothing but read computer manuals. While the level of education I've subjected myself to is extreme, the problem is that most people who are online don't have any education at all regarding how it all works and what's required to keep the bad guys out.

I'm certainly not saying licensing or certification or insurance or anything else like that should be required, but people have to take responsibility for what they do online, just like they take responsibility when they drive their car out on the road.

PepperdotNet
15 February, 2013 17:29

Reply   *Vote*

Back-doors are NOT the answer

David, the government must rationally reach the conclusion that secure encryption, with NO BACK DOORS, for private individuals, businesses, and non-profits is good policy for protecting the entire world from a conflagration that is soon to be ignited. The Tech News Article at this link-

http://blog.parts-people.com/2013/02/11/surveillance-proof-encryption-silent-circle-by-pgp-creator-a-navy-seal/

is NOT about the technology. It IS about the recent history and DESTRUCTIVE RESULTS of government back-doors into encryption software.

---Wordman
https://plus.google.com/114660584480111918841/about

Paul B. Wordman
13 February, 2013 16:56

Reply   *Vote*

Bingo!

Back doors ARE a single point of failure vulnerability. If you think we're under "constant attack" now, those back doors are a big fat bullseye!

frankzoo
14 February, 2013 15:19

Reply   *Vote*

Only the government can protect us!

That is the cry of the Left. All we have to do is give them all of our money, all of our guns, and give up all of our rights and society will be safe and perfect!

Yeah, right. History tells us what happens when people give up their power to government, and it ain't pretty. Our nation was created to keep the balance of power away from Washington, not concentrate it in a few hands. Too bad we pissed it all away.

itpro_z
13 February, 2013 16:58

Reply   *2 Votes*

| 1 | 2 | Next » |