SWCP Portal
January 2017

Like the old Cold War, only a lot weirder and confusing

World Information War, 2017

January is traditionally the *Portal*'s Annual Security Review, with a summary of emerging threats and some reminders on how to keep safe online. This year is somewhat different, for not only are the dangers greater than ever before, but the **Cold War is back** – and it is largely being fought across the internet.

Last year's US **Presidential election hack** brought this alarming situation to the attention of the world, but things have been slowly getting worse for years. While criminal hackers have steadily added exploits, **Edward Snowden's revelations** first gave a glimpse into what could and was being accomplished by the NSA and by extension, other governments as well.

Then, with the **Stuxnet virus**, cybersabotage crossed the line to wreak havoc in the physical realm. Since then, with things like the **OPM breach**, it has become increasingly clear that many outlaw hacker gangs had actually become sophisticated instruments of state conducting covert low-level electronic warfare.

In their **joint report** on the election hack, DHS and the FBI included a list of almost *50* code names given to such Russian groups. No doubt the Chinese have substantial numbers, too.

Last year **hackers** not only got into the **Democrats' email**, but the **Panama Papers** detailing how the rich hid their wealth offshore, and even twice got Facebook founder Mark Zuckerberg's **own accounts**.

> "Every practicable obstacle should be opposed to cabal, intrigue, and corruption. These most deadly adversaries of republican government might naturally have been expected ... from more than one quarter, but chiefly from the desire in foreign powers to gain an improper ascendant in our councils. How could they better gratify this, than by raising a creature of their own to the chief magistracy of the Union? "
>
> –Alexander Hamilton, Federalist No. 68, March 14, 1788

There were also a series of "**megabreaches**" found, starting with a billion passwords filched from Yahoo, and several hundred millions more credentials from MySpace, LinkedIn, Tumblr and others. While likely of minimal value to hackers unless users foolishly reused their log-ins on other sites, these were all stolen *years* before the thefts were actually discovered.

In all likelihood, there are even larger breaches and more serious intrusions that are as yet completely unsuspected. Plus, the rapid spread of the **Internet of Things**, with millions of connected but woefully insecure devices, has allowed vast **distributed denial of service attacks** (DDOS) against major American companies that run crucial internet services. Someone, the Chinese perhaps, may be practicing how to **take down the internet** at will.

Governments have **shut the net down** in their own countries over *50* times in 2016, despite the billions in lost revenues the disruptions caused. Most were ordered by authoritarian regimes involved in atrocities, but it shows it *can* happen. According to one professor, President Trump could have the **legal power** – if perhaps not yet the **technical means** – to do so here should it ever become necessary.

Meanwhile **President Obama has acted**, expelling 35 Russian diplomats, announcing sanctions, and also promising a covert response. There's also a **cybersecurity hotline**, which he is said to have already used to directly warn the Russians.

The great game in cyberspace

Cyberwar takes place in the **deep web** and the labyrinths of computer code that run the net. But war is going on across our screens as well, because cyberwar is just one part of the overall **propaganda** war, where **disinformation** is scattered everywhere to confuse and manipulate the opinions of the enemy.

It's no coincidence that many of the sites serving up fake news about Hillary were also praising Putin to the skies. **Fake news** is fake news, but it appears as if the Russian leader is employing all the time-tested tools of the **Cold War** in a modern online context.

Cold wars are, as the name suggests, warfare without bullets. They are generally of great noise but limited lethality. The reason is simple: nuclear weapons are

so overwhelmingly destructive that *no one* can afford total war. Perhaps the net is not only equally valuable but equally vulnerable.

Hackers have shown that online offense seems to be easier than defense. As soon as one hole is plugged, another is found to be exploited. Could that be due to the very nature of computers?

It seems logical that *any* electronic device sophisticated enough to receive commands, interpret, and respond to them could be wilfully *lied* to. With the internet's built-in transparency and responsiveness, it may be impossible to ever truly achieve full security.

Yet, with the immense power it harbors, and the murkiness of online attribution, **cyberspace** has become a preferred battleground for the hidden conflicts between many actors and groups. It is one of the few arenas where weak powers can strike effectively at stronger ones and likely get away with it. Yet in the post-Stuxnet world where online actions can wreck infrastructure, there never has yet been an all-out **cyberwar**. We can only begin to imagine what it might be like, but it could be quite catastrophic.

Next to that, the election hacks seem almost trivial. The **Russians scoff** while various Western **pundits** pronounced the evidence of the election hack itself "insufficient" – even the **FBI** took a long time to get onboard with the intelligence agencies – and "**false positives**" also make attribution difficult. How can they know for sure that the Russians are behind it? Maybe it's just "some guy in his home in New Jersey" as the president-elect mockingly **suggested**.

In a war of information, officials dare not reveal sources and methods to the enemy. So we may never know just what actual "smoking gun" information the spooks may have. But one of Snowden's **leaked documents** suggests that the agency could know precisely just who, how, and what were involved.

It could also be that American security services originally overlooked the low-level penetrations as minor because they were far more concerned about a **digital Pearl Harbor**. The potential of deep penetration and the unknown vulnerability of our infrastructure might be why **Obama's sanctions** seem so light to some. Yet preparations for cyberwar quietly continue behind the scenes with the president recently **separating DoD cyberwar** managers from the NSA.

Some of the promised retaliation will be **secret**. But secrecy here is a two-edged sword, for the danger of a misunderstanding is *very* high. What if, say, a power plant blows up some bitterly cold night? Was it an accident or a **Russian assault** as happened in Ukraine? And how will the Congress know when Russia's been punished enough, or even that it has?

The denier in chief

In the midst of all this, one person who was totally unmoved and skeptical of Russian involvement has been *the **president-elect** himself*. Not only has Donald Trump **praised Putin** and **criticized American intelligence** – yet another absolutely unprecedented and baffling feature of this situation – but by doing so, he put himself at odds with **17 US intelligence agencies**, the **US Congress**, his **own party** and even his own **top cybersecurity advisors**.

Perhaps this and Trump's other radical proposals are negotiating ploys to set up positions he will be willing to later modify as he might do in business. Yet there are other possibilities that are very disquieting.

To identify the culprits, the ancient Romans, who knew a thing or two about political conspiracies, would ask "*cui bono?*" – **who stands to gain?** They might not be surprised that the citizen who most dismissed any foreign influence on the election is also the one who would have **benefitted** from it.

What is to be done?

How this will all end up is anyone's guess, but bad outcomes could range from all the way from another administration where little gets accomplished due to internal divisions to a full-blown constitutional crisis to nuclear war. At the very least, it seems that **Cold War II** will continue, if not against the Russians, then the Chinese, as well as ISIS, Iran, North Korea, etc.

Against these adversaries, the average American can do nothing. So we are given the modern equivalent of the old "**duck and cover**" advice – change passwords often, never reuse them, don't open attachments in emails, and so on. In other words, be vigilant, mindful, and ever cautious when online.

Perhaps the best thing ordinary users can do is to be sure to **back up your data**, on flash drives, disks, or **SWCP's BUS**. Having an up-to-date **emergency supply kit** as one should do for other potential disasters would be a good idea, too. Contact us with questions or concerns. We'll be watching developments as best we can, because we're all in this together.