The CyberAdvisor – MAY LETTER

Hi,

In the CyberAdvisor letter from April 2018, I wrote: **"Are the Russians in Your Router?"** Then in May; **"If Your Alexa Wears a Babushka."** Nobody got the joke.

Last Sunday's 60-Minutes segment made the point more directly:

The Growing Partnership Between Russia's Government and Cybercriminals

The image is Leslie Stahl in shock and awe as she faces an attack map of Russian-sponsored cyber-attacks against the U.S. You can see from the volume of attacks by Russian political and criminal forces that their targets include much more than the Pentagon, political parties, and Fortune 100 companies.

It's small targets they're after, and today the casualties of large-scale cyber conflicts are individuals, homes, offices, and small businesses.

U.S.-U.K. Warning on Cyberattacks Includes Private Homes

New York Times, Apr 16, 2018 by David D. Kirkpatrick and Ron Nixon
LONDON — The United States and Britain on Monday issued a first-of-its-kind joint warning about Russian cyberattacks against government and private organizations as well as individual homes and offices in both countries, a milestone in the escalating use of cyberweaponry between major powers.

Ciaran Martin, chief executive of Britain's National Cyber Security Center, said Russia had targeted "millions" of devices in both countries, often seeking to hack into individual homes or small businesses or to control their routers.

So why are joint forces from Russian political, military, and criminal syndicates putting their bullseye on small targets? Well, for them, it's war. And because compared to every other approach to war it's easy, effective, cash-flow positive, and scalable.

See the clip below for a summation of the 60-Minutes segment. Nation-state sponsorship of cybercrime as a measure of war is a big deal and speaks to one of our democracy's greatest challenges ahead.

It's War

War means no rules. Lines are blurred, and all alliances are legit. Each party to a side contributes their strengths and resources to defeat the common enemy. The victors of battle claim the spoils, and the march to ultimate victory resumes. Cyber is like any other war - if only in these ways.

The 60-Minutes headline about the Russian cybercrime alliance is alarming but predictable. The country's political machine, military complex, and criminal syndicates form a natural partnership in their assault against the U.S.

"Knowing how to conquer is the first step, building the alliances to get it done is the second."

Sun Tzu - The Art of War

Forming alliances is the first step to war. Today, with Russia's organized ring of cybercriminals, it's open season on Americans. They're positioning to wage cyberwar for many years to come, and they fully intend to win.

As an Obama administration national security official told "60 Minutes":

"Increasingly, you cannot tell which is which when it comes to the criminal and the intelligence agency."

Lesley Stahl reports. Air Date: Apr 21, 2019

What's Next?

Battles are fought where people and money intersect. That's where you do the most damage and claim the greatest riches. In the digital age, the battlefield is on every corner of the internet. It's everywhere people, money, and internet-connected technology meet.

Increasingly, state-sponsored cyber-attacks will aim at small targets and relentlessly barrage individuals, homes, offices, personal networks and small businesses with all manners of risk - physical and digital. The perpetrators will use increasingly sophisticated military-grade digital weapons in the face of a mostly defenseless enemy, and the damage will be vast.

Making it worse, soon the frontlines of our cyberwar will grow further in scale and complexity as North Korea, Iraq, China, and others provision their respective regimes for fitness in combat on the cyber-battlefields ahead. They understand this is their moment and there will not be a second chance.

"Sometimes you simply have to wait for a change in circumstance and what was impossible then becomes probable."

Sun Tzu - The Art of War

How you come out of the next five years of a global rout by cyber warfare and crime will depend a lot on how you position yourself today.

What To Do

Don't underestimate the stakes of rising digital risk.

"How you come out of the next five years of cyber warfare and crime will depend a lot on how you position yourself today."

And remember - underestimating the ferocity of digitally-propelled change is the hallmark of most failure in our age.

So, here's what to do:

First and foremost, think differently. It's the adaptive that survive change and succeed. So, face the change head-on and commit to evolving and strengthening your digital sensibilities. Think of it a life-skills for the digital age. It's empowering, and you will want to share your sense of resiliency and self-determination with others.

Seek autonomy. Digital autonomy - start to draw some lines between yourself and Big Tech, Big Government, and Big Business. It's more than just doable, it's liberating. An example is email. No one but you should own your email. Privatize your email and you've created a fortress that will protect all elements of life for the rest of your life.

Cybersecurity for Life - Our byline. Cyber risk is existential; everywhere all the time. Choose tools and practices that serve and protect you, your life, and your everyday technology. Survival in the digital age is not about an IT department, the government, or law enforcement. It's too late for that. It's about you and the choices you make.

Finally, yes it's true. The Russians really are in your router. And in your devices, and email. And you shouldn't be surprised if you see your Alexa in a babushka any time soon.

Thanks for reading,

Brad Deflin