Cybersecurity is a Racket

by Jiminy Cricket

April 20, 2025

A racket, so you know, is "a service that calls forth its own demand, and would not have been needed otherwise." By that definition, most major industries today are rackets, including healthcare, insurance, national defense, public safety, higher education, and so on. I'm here to tell you we can add one more burgeoning industry to that list.

Here's what Google AI tells us:

> The cybersecurity industry is experiencing substantial growth, driven by increasing cyber threats and the need for robust security solutions, with a global market projected to reach $578.2 billion by 2033.

Why they picked that particular year on which to base their projections, I think you know. Point being, cybersecurity means big money. In today's world, nothing gets to be big money by accident. The economy is just a giant cart pulling the horse, with the billionaire and trillionaire families hidden behind private equity and investment groups creating and inflating new markets with Monopoly money. Information technology is a prime example of that, and cybersecurity is just the latest phase. It's analogous to the physical security market. You've seen smart cameras popping up at traffic lights and public squares and school campuses all over your city; how did they ever justify that expense to the public? By staging fake events like mass shootings, of course. We need only apply that logic to the digital world to make sense of the rapid rise of the cybersecurity industry.

I offer a single fact, courtesy of Wikipedia, to substantiate my claim:

> **55 percent of data breaches are caused by organized crime.**

Miles has already shown that organized crime was entirely an FBI creation. Hoover created the American mafia from whole cloth and sold it to the public in order to justify a massive expansion of the FBI's budget. So to see organized crime responsible for over half of all data breaches just means that your own government officials—and your own tax dollars—are stealing your data. But wait, why would they need to do that when they already have full access to all of your data via cozy partnerships with Google, Intel, Microsoft, Apple, etc.? In other words, why would the trillionaire families have to steal data they already own? The only answer that makes sense is that they are trying to sell their latest scam: cybersecurity.

To be clear, I'm not saying all cyberattacks are perpetrated by your own government. I am saying all the *major* ones are, and probably most of the minor ones, too. And most of the hackers out there are in the employ of national intelligence, whether they realize it or not. Check out this illuminating post on Quora from an NSA analyst who admits that the NSA tracks down hackers globally, not to hand them over to the FBI, but **to recruit them**.

But let's dig deeper. One of the largest cybersecurity firms in the world is Palo Alto Networks.

> The company serves over 70,000 organizations in over 150 countries, including 85 of the Fortune 100. It is a partner organization of the World Economic Forum.

Big red flag there already. The WEF is not in the business of protecting personal rights or privacy, so why would they want to partner with Palo Alto Networks? Because the WEF is really about engineering the global economy for the trillionaires' maximum profit, and cybersecurity is one of their latest high-margin markets.

> Palo Alto Networks was founded in 2005 by Nir Zuk, a former engineer from Check Point and NetScreen Technologies. Zuk, an Israeli native, began working with computers during his mandatory military service in the Israeli Defense Forces in the early 1990s and served as head of software development in Unit 8200, a branch of the Israeli Intelligence Corps.

Another huge red flag, isn't it? One of the founding fathers of cybersecurity came out of Israeli military intelligence, which is to say *American* military intelligence. They are one and the same, you know. It reminds us of how Google was also created by U.S. intelligence via the CIA's investment arm, In-Q-Tel, and how the entire internet was a DARPA project. Speaking of Google:

> In June 2018, former Google and SoftBank executive Nikesh Arora joined the company as Chairman and CEO.

There are no Google executives who are not on the U.S. intelligence payroll, which indicates Palo Alto Networks is just another CIA or DoD front. The President of Palo Alto Networks is BJ Jenkins, who previously worked at EMC Corporation. EMC was a big-time data storage, cybersecurity, and cloud computing company founded by Richard Egan. Where did Egan come from? Before founding EMC, he was on the team that helped develop Project Apollo memory systems for NASA and also worked at Lockheed Martin and Intel.

Another big cybersecurity firm is Crowdstrike, which was founded in partnership with the private equity firm Warburg Pincus. They come from the infamous Warburg banking family, who were Venetian Jews and one of the wealthiest families in the world going all the way back to the 1500s. Two of Crowdstrike's top executives, Shawn Henry and Steve Chabinsky, are former FBI officials. Are you starting to get the picture?

We can go back further. The first commercial antivirus software was developed by John McAfee. Remember that guy?

He tried to run for president on the Libertarian ticket in 2016 and 2020, which goes to show what a joke the Libertarian Party has become (if it was ever *not* a joke). Tim Dowling has McAfee's genealogy up at Geneanet, where we learn he is a Ball, Locke, Atherold, Waltham, Croxdale, Webb, and Hathaway. That makes him a relative of George Washington, King Charles, and Anne Hathaway, among many others. The Webb line takes us directly back through de Richmonds and de Burghs to the Plantagenets, meaning he is European royalty. He was also born on a British U.S. Army base, and his mother is English, so the royal blood is likely even more recent. He worked for NASA, Lockheed, and Booz Allen Hamilton before starting his antivirus software company—all major red flags. McAfee allegedly died in 2021, but his own ex-girlfriend claims he faked

his death. Do you think that bozo was ever involved in anything real? His whole life, including his death, was a scam, and that goes for his antivirus software, too. Anyone who ever had McAfee software on their computer knows it acted more like a virus than an antivirus, slowing your computer way down and bugging out constantly. But I don't mean a scam in that way. I mean the whole virus vs. antivirus war was controlled from both sides, just like physical wars. So the move from defense contracting to antivirus software makes a lot of sense.

Can we tie major cyberattacks back to U.S. intelligence? Of course we can.

> The **WannaCry ransomware attack** was a worldwide cyberattack in May 2017 by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It was propagated using EternalBlue, an exploit developed by the United States National Security Agency (NSA) for Windows systems. EternalBlue was stolen and leaked by a group called The Shadow Brokers a month prior to the attack.

Wikipedia is writing my paper for me at this point. One of the biggest cyberattacks in history used an exploit created by the NSA, yet we are supposed to believe the NSA had nothing to do with the attack. But wait, why would Microsoft allow the NSA to create its own private back door into its operating system? That is explicitly what Wikipedia tells us. The obvious answer is that both Microsoft and the NSA are simply different departments of the same company. And how on-the-nose is a group calling themselves "The Shadow Brokers"? They might as well call themselves The Hidden Hand of Phoenicia or The Isle of Man Bugbears. But who are they?

> The Shadow Brokers (TSB) is a hacker group who first appeared in the summer of 2016. They published several leaks containing hacking tools, including several zero-day exploits, from the "Equation Group" who are **widely suspected to be a branch of the National Security Agency** (NSA) of the United States.

See the merry-go-round they are creating for us? WannaCry used an NSA exploit leaked by The Shadow Brokers, who actually leaked it from the Equation Group, who is actually the NSA. But it gets better, since Wikipedia tells us it is The Lazarus Group who is suspected of being behind WannaCry. They're the ones who actually used the leaked exploit from TSG/Equation to perpetrate the attack. A "leaked" internal NSA memo tells us that Lazarus comes out of North Korea. However,

> Kaspersky also acknowledged that the repetition of the code could be a "false flag" meant to mislead investigators and pin the attack on North Korea, given that the worldwide WannaCry worm cyberattack copied techniques from the NSA as well.

They're basically admitting the NSA was behind it all. The Shadow Brokers, Equation Group, and The Lazarus Group are all just codenames for NSA. It takes less than half a brain to figure that out.

Park Jin Hyok is one of the alleged masterminds behind The Lazarus Group.

That's the only photo we get of him, and it reeks of CGI. His clothes don't look real, as if they're some sort of AI composite. North Korea denies his existence, which is a little inside joke, since they're actually telling you the truth. Park is on the FBI's Most Wanted list, which just tells you he is an intelligence asset or ghost. **Everyone on FBI's Most Wanted is an agent.** That's true whether he exists or not. At this point it's probably easier for them to AI-generate all their criminals, since using real people runs the risk of them blabbing at their retirement party after a few too many glasses of Moët. Park and The Lazarus Group used ransomware to extort $81 million from the Bangladesh Central Bank in 2016. Sure, because why ask for an even 80 mil when you can demand 81? How else will they get their Dead Man's Hand in there?

Here is some more pretty explicit evidence the NSA is behind cyberattacks:

> The Office of Tailored Access Operations (TAO), now Computer Network Operations, and structured as S32, is a cyber-warfare intelligence-gathering unit of the National Security Agency (NSA).

Via TAO, the NSA has admittedly created several cyberattack methods, including QUANTUM. Why would the NSA, who is supposedly trying to prevent cyberattacks, be creating the ransomware that enables them in the first place? It gets better:

> Microsoft provides advance warning to the NSA of vulnerabilities it knows about, before fixes or information about these vulnerabilities is available to the public;

> this enables TAO to execute so-called zero-day attacks. A Microsoft official who declined to be identified in the press confirmed that this is indeed the case, but said that Microsoft cannot be held responsible for how the NSA uses this advance information.

We are told these attacks are used on foreign entities. Okay, but why would we just take the NSA's word for it? Do we really think their word means anything? It's just a bald claim with no proof, like everything else the NSA tells us. Remember, we just saw them blaming WannaCry on North Korea when it's covered in the NSA's own fingerprints. But you see how this explains the mechanism by which the NSA can perpetrate cyberattacks on the American public: Microsoft tells them about vulnerabilities before they fix them. But we already caught them admitting the NSA creates those back doors themselves with Microsoft's blessing, which means we've caught them in a major lie here. You can't pretend to be vigilant about finding vulnerabilities when you allow other vulnerabilities to be built into your product in the first place.

Speaking of North Korea, let's not forget that entire country is just a front for U.S. intelligence. You might remember this photo of the main mission control center for their space program:

Their space program wasn't launched until 2012, but apparently they could only find computers from 1985. Of course, nothing you see on any of those screens means anything, and those men in white lab coats (why lab coats?) are just paid actors. Do you think North Korea also has a room like this full of hackers? Are they also wearing lab coats? Well, actually:

No lab coats, but we do get a man drawing the North Korean flag in Paint on a state-of-the-art Windows 95 PC! That's the lead photo in a 2013 *Wired* article titled "Pentagon Warns North Korea Could Become a Hacker Haven". Yeah, we're all shaking in our boots. Here's the first line of the article:

> North Korea is barely connected to the global internet. But it's trying to step up its hacker game by breaking into hostile networks, according to a new Pentagon report.

Oi Vey, the things they expect us to believe! Here's another laugh for you:

"After an intense birdwatching session, Kim Jong Un and his gaypals catch up on season 3 of *Will & Grace*."

How about that big Equifax data breach—remember that? Here's Wang Qian, one of the four PLA masterminds behind it:

They couldn't do any better than that? Pathetic, guys.

Another well-known computer worm is Stuxnet. Wikipedia tells us Stuxnet is believed to be responsible for causing substantial damage to the nuclear program of Iran.

> Although neither the United States nor Israel has openly admitted responsibility, multiple independent news organizations claim Stuxnet to be a cyberweapon built jointly by the two countries in a collaborative effort known as Operation Olympic Games.

Funny, isn't it, how behind every door where we'd expect to find some malicious and shadowy hacking group, we find our own intelligence agencies, instead. And since the nuclear program of Iran is about as real as North Korea's space program, we can peg all of this for what it is: *fake* attacks on *fake* enemies to extort *real* money via the U.S. Treasury. This is racketeering at its finest. The NSA creates the problem so that it can sell a solution:

> The idea behind the defense in depth approach is to defend a system against any particular attack using several independent methods. It is a layering tactic, conceived by the National Security Agency (NSA) as a comprehensive approach to information and electronic security.

In other words, your company needs to spend hundreds of thousands of dollars each year on multiple IT security layers; the more "robust" (read: expensive) the better. That's where firms like Palo Alto Networks come in. To bring this all home, can you guess who the top shareholders of Palo Alto Networks are? That's right: Vanguard,

Blackrock, Morgan Stanley, State Street, and Bank of America. Same for Crowdstrike: Vanguard, Blackrock, State Street, and Morgan Stanley. These are the investment groups of the trillionaire families that also control the NSA, the FBI, the CIA, and even all the huge "public" corporations that are being "hacked". That's why most of these ransomware attacks demand bitcoin—it's the intelligence community's native currency, so it's more convenient and keeps it off the books. And if a large company must pay a ransom, it's just robbing Peter to pay Paul, since both the victim and the attacker are part of the same family holdings. Unless it's one trillionaire family attacking another, which is possible. But in that case, the families aren't burdened by the increasing costs of cybersecurity—YOU are. Companies just raise the prices on their goods and services to cover additional G&A costs, and that includes cybersecurity. As usual, you the consumer and taxpayer are left holding the bag.