Invited Address

Mr. Jose Sancho
Chairman, Panda Security
Technology Partner

Since I am not a researcher and I do not belong to a defense institute, my view on cyber security comes from the perspective of an entrepreneur in a cyber security company.

First, the origin of cyber attacks has to do with digitization. Digitization is everywhere. As individuals, companies, or states, we all use it. The only difference is in its applications. Individuals use it for digital cameras, maps, alarm clocks or newspapers; companies use it for marketing and sales and for customer support; states use it, for example, for tax collection or elections.

So, everyone—people, enterprises and states—utilizes digital applications and these entities compete against each other: people compete against people for promotion in a company, for wealth, or for vanity reasons; enterprises compete one against the other for market share; states compete for gross domestic products and income per capita.

Since all compete for wealth, who wins the competition? Those who have more productivity. In the past 20 years, 80% of the productivity increase has had to do with IT, meaning hardware, software or communications. Although these seem like three very different things, all are based on software and, by definition, software is vulnerable. Even the most powerful computer, a quantum computer today, cannot thoroughly test just one program with 1,000 lines of code.

There are freelancers in the market who seek bugs in the software. They sell the bugs they discover on the free market.

If you think of an IT application, such as autonomous cars, they have 100 million lines of code. It is impossible to thoroughly test that software, which is the reason why software production companies have more people in quality assurance than in software development.

As part of the software ecosystem, there are freelancers in the market who seek to find bugs in the software. These freelancers sell the bugs they discover on the free market and some of them are even listed companies. Zerodium is one of them. It is listed as a Nasdaq company and is a market place for holes in the software. Quite often, the software producer, like Microsoft or Cisco, will plug the bugs, but at other times, companies or states will use these bugs to implement malware.

Malware and hacking are the sources of cyber attacks which are the criminal way to get wealth in a digital world.

Another source of cyberattacks is theft of identity and impersonation. Malware and hacking are the sources of cyber attacks, which are the criminal way to acquire wealth in a digital world. It is a new type of delinquency that has appeared because of digitization.

Who are the attackers today? There are three different families of attackers. The two biggest ones are the U.S. and China, because they have the most resources. Cybersecurity service companies in the U.S. that are listed on the Nasdaq employ 250,000 people that are dedicated on a full-time basis to U.S. intelligence agencies.

In China, the situation is less transparent but taking into account only what listed companies report, we can guess that China has even more people than the US who are dedicated to cybersecurity and with a more blurred line between state and enterprise.

Countries like Russia, Iran, or North Korea have an interest in influencing swing voters in elections.

The key point is that you need cooperation between governments, enterprises and industries. In the military, there is a similar situation for combat aircraft that are produced by engineers and operated by soldiers and for cyber weapons that are produced by hundreds of thousands of engineers. Of course, other actors can also buy cyber weapons on marketplaces. These marketplaces include stable countries like Russia, Iran, or North Korea that have an interest in disturbing other countries—for example by trying to influence swing-voters in their elections. Because of all the information available to them, they know exactly who the swing voters are and what kind of messages they are sensitive to.

Those states attack others. Actually, a major target is Europe which has the second largest concentration of wealth in the world, and is not well organized and structured. To give you an example: last year, one European country suffered 110,000 attacks as reported to its national CERT. Of those 110,000 attacks, 1,000 came from the intelligence services of other states and they were directed to very specific public administration or defense institutions. Some of these attacks have been reported in the media.

Many attacks are based on cheap weapons, like WannaCry or Petya that have been stolen from the biggest states.

So, out of the three types of actors, the two biggest ones are states using cheap weapons. Other actors, enterprises or individuals, are the authors of these 110,000 attacks that I mentioned above. The vast majority of these attacks are for profit and many of them are based on cheap weapons, like WannaCry or Petya, which have been stolen from the biggest states.

What is the defenders' landscape today? Since attackers have a huge advantage, what can defenders do on their side? We have products like the ones my company produces, but the typical software development takes at least three years and our laboratories detect more than 100,000 new malware samples every day. That means that every day, the malware producing industry is growing faster than the speed at which we can produce software. The other characteristic of these products is that they are global. Once you have a product, you have the means to defend against all the malware coming from that source at that time. This market is worth $35 billion per year in revenue.

Before 9/11, it seemed impossible to fight against money laundering because people were behind rogue states.

The other side of the industry is services. As it takes three years to develop a new product and new attacks come daily, we need services based on people in order to prevent and defend against those attacks at the local level. Globally, that market is about $45 billion, which is larger than the products' market. In terms of people, it means 600,000 people working in services. I think that China has more than that and the U.S. is probably on the same level as China. We know for sure that it is at least 250,000 people. This gives you an idea of why we have attacks, what the landscape is for attackers, and what defenders can do.

How can we progress towards making that situation more controllable? An analogy should give us an idea on how to proceed. The analogy is money laundering. We need a trigger and the trigger for dealing with money laundering was 9/11. Before 9/11, it seemed impossible to fight against money laundering because people were hidden behind fake enterprises and theoretically resided in rogue states. If you have access to the whole chain of money, however, it seems impossible for one autonomous state to go to war against another.

In response to money laundering, the key words became "last beneficial owner." The tax authorities want to know who is the last beneficial owner, who is behind the enterprises, who is behind the states? The last beneficial owner is the one getting the money and putting it into his pocket. Who is the last beneficial owner of Facebook? Probably Mark Zuckerberg. Even if you buy 99% of the shares of Facebook, the one who will give the orders at Facebook will be Mark Zuckerberg because that arrangement was established at the time of the IPO. Who is the last beneficial owner of Google? Larry Page. It is very clear in the by-laws of the company. If you can find the last beneficial owner and follow the chain, you will find the enterprise, the IP address, the telco operator and the state. This chain in cyberattacks is analogous to the money laundering one. Of course, we will need specific legislation to make it possible to follow the chain and the capability to enforce those laws.

If you can find the last beneficial owner and follow the chain, you will find the enterprise, the IP address, the telco operator and the state.

So, in my simple view, what is the way ahead? It is again based on another analogy which is deterrence in nuclear weapons, which is achieved by global cooperation among states. We have to uncover the delinquent IPs behind the companies and behind the last beneficial owner. For people, there are laws, penal laws and criminal laws; for companies, there are mercantile laws; and for states, international laws. Adequate laws need to be applied in each case. We also need to regulate telcos and social and advertising companies related to security or manipulation issues. I do not think it is easy, but it is feasible with today's technology.

We need to regulate telcos and social and advertising companies related to security or manipulation issues.

To continue with this analogy, we need global cooperation, mutual reciprocal monitoring surveillance and we need to enforce the laws. How long will that take? Over the last five years, every Sunday's *Financial Times* has advertised houses for sale in the Isle of Man or in the Bahamas. The reason for that is very clear: the Bahamas and The Isle of Man require physical residence over 50% of the time to benefit from the laws that shelter their residents. So, this shows what tax evaders have to do. And is there is legal enforcement to prevent it? How long will it take for us? Fifteen or 20 years? Of course, we need a trigger and WannaCry was big but not big enough to provide the necessary trigger. I am not saying that we need an equivalent to 9/11 but we do need a trigger. If we have that trigger, we will probably be there in 20 years.

The EU is important, but the big states in it are probably more important: Germany and France, as well as, Italy and Spain.

To conclude, what should Europe do in the meantime? First, in Europe today, we are probably without influence because the biggest actors, China and the U.S., can act with one single voice. In Europe, that single voice does not exist. First, we need that cooperation between states and enterprises. The EU is important, but the big states in it are probably more important, they are the tractor ones. By that, I mean Germany and France and, on a secondary level, Italy and Spain. As to the UK, let's see what happens with Brexit: the UK could be very important for cooperation between states and enterprises.

As point number two, we need to achieve leverage through our products. Of course, the U.S. has more people than the whole services industry together, and in products, they have 80% of all the product revenue. And the last beneficial owners of these companies reside in the U.S. and they are governed by U.S. legal rules. So, we have no equivalent to the level of strength that the U.S. or China have with Huawei or Qihoo. We need leverage for our products.

Another point is that, in Europe, we need to lift some constraints that we have on budgets. If a company wants to win a bid to supply a public administration, it probably has to fight on the basis of price against American companies who will know better than us how to win in this context. So, we need cooperation. There is a clause that can be used for cooperation, a national security clause, but it is very rarely applied in Europe. We need to fight for it to be used, because you have to keep in mind that the root cause for cyber-attacks lies in a human condition that will always be there. Because software will be there, hackers will be there. That human condition is greed, and the only way to counterbalance that greed is to be linked to another human condition, which is fear.

In Europe, there is a rarely-used national security clause that can be used for cooperation, and we need to fight for it to be used.