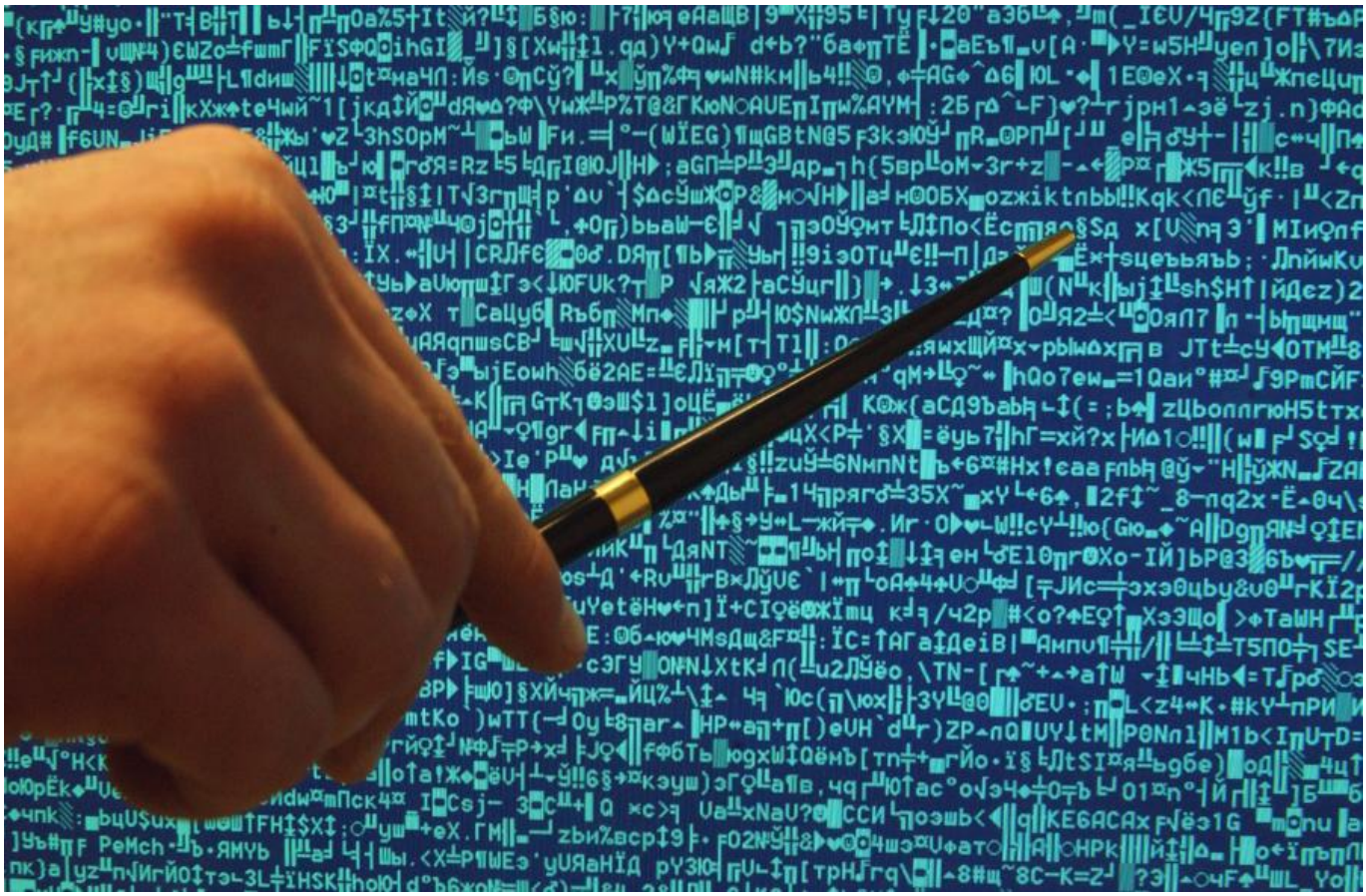
Page source: http://intersectionproject.eu//article/security/implausibility-patriotic-hacker

INTERSECTION
RUSSIA / EUROPE / WORLD

- Author: Nikolai Holmov

The Implausibility of a "Patriotic Hacker"



By suggesting that "Patriotic Hackers" could be behind large-scale cyber attacks, Vladimir Putin was being mischievous and perhaps bordering on the absurd. The quantity and quality of attacks on Ukraine over the years in most cases rules out the possibility of anyone doing this simply as a nationalist hobby

Proving who is behind a cyber attack is hard. It is even harder to prove if there is anyone pulling the strings of whoever is behind an attack. A recent cyber attack on Ukraine - nicknamed 'notPetya' - brings this difficulty of attack attribution into sharp relief. On the morning of June 27th, Ukraine's banks, government ministries, media organisations and other key infrastructure points were hit by an apparent ransomware virus, effectively encrypting whole databases and holding them hostage in return for money. Experts, however, concluded that financial criminal gain was probably not the real motive, hence the attack code was named "notPetya" despite the cloak of a preexisting ransomware called "Petya". It looked a lot like simply causing hassle and disruption in Ukraine was the real prize for these attacks the day prior to Ukrainian Constitution Day. However the ransomware quickly spread beyond Ukraine's borders, affecting over 60 international organisations around the world.

Ukraine has blamed "notPetya" on Russia, just as it did the cyber attack on its 2015 elections. Similarly, the Ukrainian government has pointed the finger at Russia following cyber attacks on its vital infrastructure in

2015 and in 2016. Despite attribution itself being difficult and time consuming, this accusation would of course make contextual sense, given that Russia and Ukraine are locked in conflict that extends beyond the illegal annexation of Crimea or the occupied Donbas region. These attributions of Ukraine eventually seemed to get the backing of many experts. Experts, to be fair, will not rush to attribute cyber attacks, for attribution credibility matters.

These rare public moments where an attack succeeds in causing system damage or significant financial losses creates a false impression that cyber attacks are deployed only occasionally. The reality of cyber war is much more constant between Russia and Ukraine. It is similar in intensity to the ongoing battles along the physical frontlines in eastern Ukraine, and the other ceaseless types of conflict involving espionage, diplomacy, economic tools, and propaganda.

Like these other aspects of war, cyber attacks are unlikely to end any time soon. Thus it is worth reflecting on how credible attribution can be improved, and how we can all get a keener sense of what is achievable in the cyber world without entering the realms of any possible, a 'nuclear option' that a state or organisation can resort to. How can any existing deterrence be more convincing and defenses significantly improved? What can realistically be achieved by an individual, or a team, why, and at what cost? In the ever converging gap between terrorism, organised crime, State and quasi-State actors in cyberspace, can credible attribution be made and if so, what action to then take as retribution besides simple symmetric retaliation?

President Putin has recently mentioned "Patriotic hackers." These are everyday Russians who, Putin hints, may have done a bit of hacking here and there in what they believe to be the Russian interest, but are nothing to do with the Russian state. The most notable action that "Patriotic hackers" have undertaken, Putin alluded, was their possible involvement in the US elections hacking the servers of the Democratic National Congress.

APT 28, also known as Fancy Bear and APT 29, also known as Cozy Bear, are the most regularly, but not only, touted labels for various Russian secret services engaged in cyber misdemeanors by the international media.

"Patriotic hackers" however are unlikely to equate to the abilities of an APT.

The difference is not a matter of coding ability. It is a matter of a combination of will and *mens rea* over a sustained period of time. The clue is in the name - APT stands for Advanced Persistent Threat.

Just how persistent is a "patriotic hacker" in comparison to a real, usually State or State-sponsored APT?

In order to ponder that question, it is perhaps reasonable to try and construct a theoretical APT, for it is not a software or cyber-realm tool. An APT is people - it is not one person. There is structure and there is process. There is a goal and perhaps a customer for the specific product. Therefore an APT begins with people - plural. Then come the ideas and targeting. Lastly comes the very clever computer wizardry to achieve the desired nefarious goals and/or outcomes - whatever they may be.

So how to conceptualise, or at least try to visualise, an APT when looking past the *en vogue* phrases of zero day exploits, toolchains, hacks, and implants that make for gripping media copy? In a more mundane real world, it is people who have to develop, research, use and maintain the toolkit for cyber mayhem. There is a requirement for operators, developers and systems administrators keeping everything up and running the entire time any particular designed cyber event is on-going, and to further develop the next cyber tools for the next cyber operation as new ideas germinate.

Even if we assume a "Patriotic hacker" is able to multitask and perform brilliantly with an extremely wide and varied set of skills, already this begins to move beyond the ability of a single "patriotic hacker" doing this as some sort of hobby.

There is then the matter of having the untraceable, (or at the very least extremely difficult to find), infrastructure upon which to run and test out all of these clever exploits. Easy attribution may bring a smirk when hacking elections, but is not necessarily desirable when crashing financial systems, shutting down national infrastructure, and possibly committing acts that could be deemed casus belli or, possibly, war crimes. Just like bombing raids, it takes a lot of training to make sure that malware hits the precise target and avoids unintended damage and wider repercussions, yet both can and sometimes do cause unintended

collateral damage.

There is also the question of payment. If the APT is comprised of numerous "patriotic hackers" pursuing either criminal or State ends, then somebody therefore has to create numerous shell companies, bank accounts and legal cutouts to make attribution and/or criminal responsibility extremely difficult. Such skilled legal gymnastics are probably not easily within reach for an individual patriotic hacker.

However, having successfully and cleverly penetrated the target's system, having created numerous shell companies within shell companies, and on the *proviso* that the exploit is to extract data rather than simply damage and degrade the target system, there will need to be analysts for the megabytes or terabytes of exfiltrated data.

A lot of analysts if the exfiltration is on a massive and perhaps on-going scale.

Analysts fluent in the national language of that exfiltrated data. If not, then translators will be required too. The APT personnel requirement continues to grow if it is to achieve its goal in a timely and efficient manner providing anything approaching a quality illicit commercial or State espionage product. A raw data dump is not the best way to make money, nor does it provide the most useful of intelligence product for a customer.

With the requirement for numerous analysts, so too grows the amount of IT hardware and (very expensive) IT analytical software. So large may be the amount of exfiltrated software that it may be necessary to develop in-house analytical software to cope with the quantity.

There is also a requirement for somebody to manage this APT to prevent mission creep, deal with "patriotic hackers" going sick, losing interest, or getting another project that pays very well - and all the skills and roles mentioned thus far have a global commercial remuneration that provides for a very reasonable lifestyle. There is competition for such people.

Patriotism is all well and good, but a "patriotic hacker" has to pay the rent and feed the family.

Consideration too, is to be given to any genuine outsourcing by the State when it comes to control of exfiltrated data. How much, if any, of an APT structure can be outsourced without creating unnecessary risk? The "on-hire" personnel costs of all the above skill sets of sufficient number to produce a timely and quality product from the commercial marketplace would probably run into $ millions per year - or alternatively equate to similar losses for a team of "patriotic hackers" working pro bono for a State actor (unless coerced to do so).

We have perhaps now reached the point where theoretically it becomes clear that a "patriotic hacker", or even a few "patriotic hackers", would struggle to meet the "Persistent" requirement in the Advanced Persistent Threat (APT) definition – at least without significant support.

Even if the target employs poor cyber security that might allow for some easily accessible hacking tools to be used, and even if there is a mole within the target organisation that can assist the analysts, the "patriotic hacker" association with, and as a ruse for a State or State sponsored APT is, well, not particularly apt.

Quite whom Presidents Trump and Putin had in mind for the muted, quickly dismissed bilateral “impenetrable” cybersecurity unit is unlikely to ever be known – perhaps President Putin was aware of some Patriotic hackers with some free time?

Tags
cyberwarfare
hacking
military
Category
Security