Patriotic Hackers in Cyberspace Operations: Independent or Sponsored Cyber Actors?

Drioueche Asma Sarra Youssra,

The National Post Graduate School of Political Sciences (Algeria)
, drioueche.asma@enssp.dz

Received: 02/03/2022 *Accepted: 22/03/2022* *Published:06/06/2022*

Abstract:
Technological advances have allowed actors other than states to engage in cyber activities and even conduct cyber-attacks. Examples of these actors include hacktivists, cyber criminals, and patriot hackers. Each one of these actors has a specific aim to achieve, in some cases it could be gaining money or fame or defending social causes and in other cases it could be acting out of nationalism to protect the interests of their state which is the case of Patriot Hackers.
This paper examines how relatively new non state actors have come about in the cyber domain, more specifically patriot hackers, understanding who they are, their role in the cyberspace, the reason why they engage in cyber activities and most importantly whether they conduct these cyber acts independently or rely on a certain party to do so, i.e. their role in assisting states in the cyber domain, whether or not they have any affiliation with their government and if this latter is using them to conduct cyber-attacks to avoid attribution.
Keywords: Cyberspace, Cyber Attacks, Non-State Actors, Patriot Hackers, States.

Corresponding author**: **Drioueche Asma Sarra Youssra.

1. INTRODUCTION

The integration of computer and network systems into the critical infrastructures has upgraded their work, but at the same time it compromised their security (Johan, 2013), and enabled state and non-state actors to carry out cyber missions dealing with protest and revolution, crime, terrorism, espionage, or military operations. (Blank, 2013, p. 406)

Cyberspace almost reduced the gap between the different actors; thus, the digitalization of warfare has increased the importance of non-state actors in the twenty first century' cyber-attacks, both as independent actors and tools exploited by nation states. (Bussolati, 2015, pp. 102-126)

The abilities of non-state actors have increased during the last two decades for multiple reasons among which the lowered barriers of entry. There is nowadays an easier access to more destructive power, owing to these actors' organizational structure, their anonymity, and the vulnerabilities they find (Studies, 2017, p. 40). In fact, the variety of threats in cyberspace comes from the variety of the actors exploiting the vulnerabilities, the actions they take, and the targets they attack. There are several types of non-state actors such as patriot hackers, cyberespionage networks and individual hackers. They each have different aims and pose different threats in the cyberspace. (Schreier, 2015)

Although States are known to be the main actors in cyber-attacks, recent cases have demonstrated that non state actors can also be main players in conducting such attacks. The cyber-attacks targeting Estonia in 2007, prove how non state actors, more precisely Patriot Hackers can be key players in cyber-attacks (Johan, 2013) government websites and banks were overloaded with distributed denial of service attacks, making emergency transmissions inaccessible. In 2008, Georgian digital systems were affected by a similar attack. When analysing these cases, it showed that non-state

actors, mainly patriot hackers, did participate in those attacks. (Bussolati, 2015, pp. 102-126).

2. Understanding Patriot Hackers and the motives behind their acts:

Before diving into discussing the role of Patriot Hackers, we must understand who they are and what their objectives are in the cyber domain. An easy way to explain Patriot hackers is the following: While some individuals defend their state from opponents in the real world, using actual weapons, others defend it on the internet. Whenever there is a conflict no matter how small or big with another entity, patriot hackers conduct different kinds of cyber activities to show off their sense of nationalism. (Rens, 2019, p. 14).

There are several definitions of patriot hackers. For instance, 'Denning' defined them as «citizens or expatriates engaged in cyber state-on-state conflict ». 'Borghard and Lonergan' provided a more recent definition in which they included Patriot Hackers within cyber proxies as unorganised groups or individuals with political objectives (Wood, 2017). 'Holt and Schell' have defined patriot hackers as citizens and expatriates engaging in cyber-attacks to defend their mother country or country of ethnic origin. As for « Dinniss », he explained that they are individuals and groups motivated by national and political aims that conduct cyber-attacks (Barata, 2015). And finally, there is the definition of 'Steven Wood' who describes a patriot hacker as « someone who, with the agreement of their government or without the agreement of their government, is carrying out malicious IT acts on behalf of their country (Wood, 2017, p. 11).

In brief, patriotic hackers are individuals or sometimes even groups who conduct cyber-attacks to achieve nationalistic and political goals and revenge their nation state by carrying out cyber actions and activities.

The cyber-attacks that patriot hacking involves are carried out by hackers against states or hackers of a state with which there is a prolonged national conflict such as: India-Pakistan, China-Taiwan, Russia-Chechnya, and of

course Israel-Muslim countries. Their activities within the cyberspace are inspired by events that, according to their sensitivity, might harm and represent a threat to their state. For example, cyber-attacks conducted against Estonian government websites and banks, in 2007 were the result of the Estonian government's decision to relocate a monument of the Soviet Era (Bussolati, 2015, pp. 102-126).

Attacks conducted by patriotic hacker groups have been seen since at least since 1999 when the USA accidentally bombed a Chinese embassy; what followed it were a series of USA and Chinese patriotic hackers' actions. (Isnarti, 2015, p. 167)**.**

Patriotic hackers have strong ties towards their motherland, they could be ties of nationality or ethnicity. That is why nationalism is considered as primary reason motivating patriot hackers into conducting cyber-attacks.

« Barata » for instance considers that patriotic hackers act on nationalistic grounds and are motivated by political objectives. « Dahan » characterizes them as parochial, self-identifying by their nationalism and patriotism, at the right of the political spectrum and with little cohesive ideology or identifiable ideology beyond nationalistic rhetoric. He furthers mentions that patriotic hackers carry out cyber-attacks with the idea of causing maximum harm in any hostile interaction (Wood, 2017, p. 12).

Patriot hackers have sometimes been linked to other motives, for instance financial ones, as they are sometimes paid for the cyber-attacks they conduct whenever recruited by the government or a given company. Others have even considered that patriot hackers are driven by another motivation which is testing their hacking abilities and building a name. Other times it is about the pride of belonging to a group defending the interests and the security of their nation. (Winterfeld, 2011, p. 211)

Another confusion that generally surfaces whenever talking about patriot hackers is the similarity between them and other non-state actors mounting cyber-attacks. There is a difference between Patriotic Hackers and the rest

of cyber actors. Patriotic Hackers' motivation in conducting cyber-attacks comes from their feeling of patriotism, as opposed to other non-state actors, for instance, 'Hacktivists' who act out of political reasons, such as defending human rights which may sometimes even be against their own government (Barata, 2015).

Many thinkers such as « Owens » and « Denning » consider that patriot hackers and hacktivists are very similar actors in the cyber sphere, while other authors like « Borghard », « Lonergan » and « Seebruck » see them as very different actors. It is true that there are some similarities between patriot hackers and hacktivists, for example they conduct similar cyber-attacks such as website defacement and DDoS to assist their nation state in an unofficial manner. In addition, hacktivism can be perceived as one of the cyber activities patriot hackers engage in, the target conceives the action as hacktivism, while the attacker perceives it as patriot hacking (Wood, 2017, p. 10).

Still, the principal distinction between a hacktivist and a patriotic hacker is that the former is active towards social issues, while the latter is motivated by patriotic interests. Hacktivists might even attack their own nation state if they see that they are violating a certain social issue.

3.About the Structure and the methods of Patriot Hackers:

Another key point that contributes to understanding the role of patriot hackers is analysing their structure, their organisation as well as the methods they use when conducting their cyber-attacks.

The abilities of patriot hackers depend on their structure; they can be individuals acting on their own or highly organised groups. While the former can't add that much to the state's forces, the latter can be a huge threat, since they conduct their attacks through a sort of command and control, which is hard to end, giving that they could be distributed globally.

« Ottis » graded their organisational level according to three models; the Forum, the Cell, and the Hierarchy and in his opinion, patriotic hackers were at the most unorganised in the Forum model and their organisational

structure became more corporate/militaristic moving from there, through the Cell and eventually arriving to what he termed the Hierarchy, where the discretion and actions of the individual were subordinated to the collective group (Wood, 2017, p. 11).

Concerning the methods exploited by patriot hackers, one thing to keep in mind is that the techniques they use to conduct their cyber-attacks are not exclusively used by them, but they are also exploited by hacktivists, script-kiddies, cyber terrorists and some many other cyber actors. These techniques usually involve using sophisticated viruses, worms, and Trojans, and even though writing sophisticated malware is beyond the abilities of most hackers, there are some who can do so (Wood, 2017, p. 54).

The most well-known cyber-attacks conducted by patriot hacker groups usually include website defacements, distributed denial of service, malware attacks (Isnarti, 2015, p. 168) **.** DDoS attack is one of the most used methods by patriot hackers since the mid-1990s, which can temporarily disrupt the host's services and prevent it from responding to genuine requests and can even be used for cover for other attacks.

In some cases, such as in the one involving the cyber-attacks conducted against Estonia, the methods used to conduct the denial-of-service attacks were explained in Russian forums, gathering many hackers to give it a state-sized scale (Friedman, 2014, p. 111). In fact, even the cyber-attacks conducted against Georgia in 2008 started with series of DDoS attacks, soon after website defacement attacks were launched (Rens, 2019, p. 54).

The benefit of Distributed Denial of Service attacks lies in crippling and disabling the target networks by making them unusable, with the purpose of causing harm or to silence adversaries by making their resources inaccessible (Friedman, 2014, p. 70). Brute force attacks are also exploited by patriot hackers. They deal with the self-operating spraying of sites with probable passwords until hackers obtain entry and eventually take over the site (Nomaan Merchant, 2021).

The cyber-attack with the most impact used by patriot hackers are the ones that involve attacking a senior or a government official and stealing sensitive data from them (Isnarti, 2015, p. 167) **.** However, Patriotic hackers are less likely to use ransomware and other techniques essentially aiming at wealth generation. thus, methods inflecting damage and distress, like DDoS, are more likely to be used.

Patriotic hackers use some of the software and services provided by sites like « 0day ». giving the nature of the Dark Web, it is rather hard to know about all the sites exploited by patriot hackers. They may also sometimes use spear phishing through which they install on the target's network a software named « RAT » which stands for Remote Access Tool. This software uses the HTTP protocol for command and control (Sunil Kumar, 2018, p. 2254), considered important during an advanced cyber-attack. An example of that happened during the 2016 email hack of the Democratic party of the USA by suspected Russian patriotic hackers.

Patriotic hackers may sometimes have access to other powerful cyber weapons in order to cause as much harm as possible during a cyber-attack, targeting significant National Infrastructures. For instance, Stuxnet is a worm that was originally only available to groups directly affiliated with the USA or Israel. Nevertheless, powerful cyber weapons have been leaked into the public domain, an example is the stolen Eternal Blue exploit that came from 'The Equation Group' and was used in the WannaCry virus.

In sum, patriot hackers mostly use Distributed Denial of Service attacks, deface websites or leak data. They pick these particular methods for a number of reasons, for one they are cheap, they are also widely available and need relatively little technical skill, at the same time they solidify the force of the attacker. As for the computers exploited in their cyber-attacks, they may either be bots in a botnet army or a coordinated effort of numerous resistance members who are ready to install the needed software on their computers**.**

Regarding the steps followed when conducting a cyber-attack, the first matter patriot hackers think of when conducting a cyber-attack is

identifying the targets. Following the weaponization of the payload, for instance loading a virus into a Microsoft office file. The next relevant move is to figure out the best way to deliver the weapon, which may either be done using cyberspace or physically via a USB stick which is pricier and more difficult to achieve and perhaps a covert operative is even needed, that is why, usually only executed by those with nation-state resources (Wood, 2017, p. 54).

4. Cases of Patriot Hackers:

There are numerous examples of Patriot Hackers. Russia has a huge population of "patriotic" hackers who conduct cyber-attacks. Research conducted by the 'Centre for Strategic and International Studies' estimated that between 2006 until 2019, almost one hundred cyber-attacks, each causing at least one million dollars in damage, could be attributed to Russian hackers, among which patriot hackers (Rens, 2019, p. 5).

Russian patriot hacker groups mount cyber-attacks against foreign governments and are often involved in ethnic or identity conflicts, especially where there are Russian-speaking minorities. therefore, these types of cyber actions mainly focus on the ethno religious cyber conflicts. Indeed, Russian patriot hackers are well known for the cyber-attacks they conduct in the name of patriotic hacking, especially since their 2007 cyber-attacks against Estonia, also in 2008 against Georgia. (Herridge, 2016)

Chinese hackers are also known to be motivated by patriotism and are among the most dangerous hackers ever. Firstly, because they operate in mass, thus many cyber-attacks are conducted at the same time. Secondly, they sometimes engage in their cyber activities, mainly when it concerns website defacement, using Chinese language, meaning that for the target to decrypt their code, they would have to understand their language (Isnarti, 2015, pp. 162-163).

Some of their actions are, defacing US websites in 1999 right after the Chinese embassy was bombed in Belgrade. In 2009, they defaced

Melbourne festival film website for diffusing a documentary about Rebiya Kadeer, a Uighur leader and in 2014, they attacked Vietnamese government websites because of a border conflict between the two states.

Among the most famous patriot hackers' groups in China; there is the "Red Hacker Alliance", the "Honker Union of China" (now known as 'CN Honker'), 'Green Army', 'China's Eagle Union' (now known as 'China Will'). They all publicly announced through a manifesto their patriotic mission (Hang, Freedom for Authoritarianism: Patriotic Hackers and Chinese Nationalism, 2014).

5. Discussing the Role of Patriot Hackers in Cyber Attacks and their alleged affiliation to their government:

Now that we have an idea about Patriot Hackers, their structure and mode of operation, let's discuss their role and how they became active in the cyber domain.

An important element that contributed to the rise of non-state actors and more precisely Patriot Hackers in conducting cyber-attacks, is the fact that nation states began approaching them in the aim of securing their infrastructures from cyber threats and enhancing their cyberspace operations, by exploiting the experience, the knowledge, and the available resources of these non-state actors (Johan, 2013). This led many to argue that these patriot hackers are affiliated to their governments whenever they conduct cyber-attacks, that the states are in fact the ones behind these attacks and patriot hackers are just a tool to achieve their goals, so what would make states think of patriot hackers to fulfil their strategic aims?

Patriot Hackers are generally low cost, a quick to stand up group, considered as force multipliers, and they have a global reach (Wood, 2017, p. 13) , but one of the most appealing trait that characterizes patriot hackers is the high level of anonymity they provide to other entities like governments trying to avoid attribution and reduce the probability of taking responsibility for executed cyber-attacks, meaning that if a nation-state can

covertly initiate, fund, or control such attacks using patriot hackers, they can reduce the already low risk of political and legal implications.

This is why, the employment of patriot hackers in cyber-attacks is very appealing to nation-states or an equivalent party (Johan, 2013), since they can easily take advantage of the anonymity feature of the internet and hide within its complex design, enabling those with sufficient technical skill to remain unknown (Schreier, 2015), work above the surface, and give them the ability to deny that the attacks originated from their nation (PRESGRAVES, 2021).

Due to the attribution concern, patriot hackers are hardly ever held responsible for their attacks, since there is simply no hard proof and because digital evidence is ephemeral in nature and susceptible to manipulation (Schreier, 2015). Thus, the upside of exploiting patriotic hackers is that a government can utilize the wide-ranging capabilities it desires without being officially involved and claim plausible deniability. Without cross-border police cooperation, it is almost impossible to detect who conducted the cyber-attacks (Friedman, 2014, p. 65).

As mentioned above, the features of digital evidence pose concerns as to its reliability since it is volatile, has a short life span, and is usually located in foreign countries. The lack of accountability and attribution is also created by the limitations of the international and local laws (Schreier, 2015).

Another advantage is that nation states take advantage of the expertise, skills and resources provided by patriotic hackers. Some governments even work with patriotic hackers to look for hacking talents and create a “B-team” of cyber reserves. It happened in China in when the military apparently organized hacker competitions to recruit talented civilians, and this was when the famous hacker group « Javaphile » engaged in cyber activities like the ones against the White House website in 2000 (Friedman, 2014, p. 68).

The state's support for patriot hacker attacks against hostile targets also benefits the government in directing these hackers away from operating against the state. 'Alexander Klimburg' argues that the Chinese government exploits patriot hackers in order to control them through integration into a national defence framework (Hang, Cyber-defense Strategies for Contending with Non-state Actors:, 2017, p. 75).

Nevertheless, the conduct of cyber-attacks by non-state actors and specifically patriot hackers is certainly not risk free since they have total control on the methods used and the targets to hit which can lead to complicated implications (Johan, 2013) and deny the state which hired them in the first place from any control.

The implications of a cyber-attack carried out by a non-state actor on an infrastructure would rely on the systems affected. The most dangerous breaches would affect Supervisory Control and Data Acquisition systems (SCADA) controlling critical transportation, power, water, health care, public safety, sewer, finance, and communications systems, forcing the State to depend on manual backup systems that would reduce its efficiency. In most cases, the harm from computer breaches is temporary, but in some cases, they could result in a physical damage and sabotage which would make a cyber-attack on infrastructure more effective (Seattle).

Among other implications of the rise of non-state actors in cyber activities is the spread of international terrorist organizations, leading States to work on their policy choices within cyberspace (Hang, Cyber-defense Strategies for Contending with Non-state Actors:, 2017, p. 79). Basically, nation states are no longer the only players or even the main actors within cyberspace, technological advances have allowed non state actors to engage in cyber activity and carry out cyber-attacks and even be approached by governments to act on their behalf in a direct or an indirect manner and benefit from their expertise and skills in the domain.

Surely, the participation of non-state actors in cyber activities has its advantages such as helping states, companies and even individuals to enhance their services and protect their vital infrastructures. However, it has

certainly its drawbacks like the issue of attributing malicious cyber-attacks to a certain actor. The main concern lies in proving if patriot hackers who conducted a cyber-attack are actually affiliated to a certain entity, more precisely their government. It is hard to prove that a government is working with patriot hackers, though security experts found that many groups and individuals, for instance APT (Advanced Persistent Threat) 28, Fancy Bear and Guccifer 2.0 work with the Russian foreign intelligence service and other state agencies.

An example that demonstrates the issue of attribution is the disruption of the 2016 US election by interfering in American voter registration systems and leaking the emails from the hacked Democratic National Committee (DNC) servers, still there is little proof linking the DNC hackers to Russia. This is partially because patriot hackers do not act as official groups within the structure of the government, but rather as loose groups under assumed identities (Lokot, 2017).

Chinese patriot hackers are allegedly affiliated with their government despite the lack of hard evidence, but the relationship cannot be denied. For instance, in 2014 when I-Cloud was targeted by cyber-attacks, the Chinese government denied any affiliation with the attacks, but the cyber security expert « Alan Woodword » said that the attacks were hosted from servers located in China to which only the government had access too.

In fact, Chinese citizens share a special relationship with their authorities, they are expected to actively engage with their government, which may mean getting involved in patriotic hacking against hostile entities. China allows and supports Patriotic Hackers to conduct cyber actions against other states, however it does not organize them. Chinese Patriot Hackers independently organize attacks through websites and forums. The Chinese government communicates with Patriotic Hacker groups via public news media (Hang, Cyber-defense Strategies for Contending with Non-state Actors:, 2017, p. 5)**.**

China is well known for recruiting patriot hackers in both offensive and defensive operations. The Financial Times mentioned the existence of a Chinese web company that goes by the names of « NANHAO » and carries out defensive and offensive cyber actions.

Even Japan recognizes the significance of using patriot hackers. Keio University Professor « Motohiro Tsuchiya » stated that Japan needs to build an offensive cyber organism that would contribute to protecting the country from any outsider attack and since most of the experts reside in the private domain where they are well paid, the government should rely on patriot hackers.

The same thing occurred in India in 2011, when the Information Technology Minister « Kapil Sibal » approached what he called 'Ethical Hackers', referring to patriot hackers, to protect their networking systems. Not only that, but the Indian government even considered recruiting and even legally protecting patriotic hackers conducting attacks against hostile states.

Counting on patriot hackers is however not that safe since they can easily go off track and use their expertise to work without the authorization of their governments and even turn on them or attack an unwanted target and escalate a certain situation. It was suggested by the DIPLOMAT that governments should at least work on a norm of state responsibility for cyber-attacks coming from their country. This will ultimately lead to state-to-state negotiations (Segal, 2012).

One thing is certain, nation states no longer individually make political decisions behind closed doors. Groups and even individuals like patriot hackers contribute to shaping strategic realities.

6. CONCLUSION

There is no hard proof of whether the government is behind patriot hackers' cyber-attacks. Nevertheless, some things can demonstrate their involvement with these non-state actors. There are certain weapons and viruses that only an official authority has access to, there are servers that only a government

can launch an attack from. Another proof is the fact that hacking is not legally accepted and yet governments do not condemn those behind these acts most of the time and punish them, and even sometimes praise them as did the Russian president ‘Putin’ when asked about patriot hackers and said : «Hackers are freelance artists, they can wake up one day and start painting pictures, and then wake up another, read international news, and if they are patriotically-minded begin to make their own contribution to fighting those who say bad things about Russia » (Today, Russia, 2017)

It is obvious why a state would recruit patriot hackers, aside from their willingness to engage in cyber actions against hostile entities, the government also benefits from the plausible deniability, since it can easily target its adversaries and avoid the attribution and thus any legal repercussions.

On the other side, there are patriot hackers who beyond their nationalism that mainly motivates them to engage in cyber actions, they also gain fame and recognition, which is something most of cyber actors look for.

It's still unclear how often patriotic hackers receive underground support from their governments, but the benefit they get from exploiting these hackers is undeniable, even though it has also drawbacks, since matters can blow out of proportion and even be turned against the state.

7. Bibliography List:

Barata, N. J. (2015). *"PATRIOTIC HACKERS": NON-STATE ACTORS FIGHTING WARS FOR STATES.* Aveiro: University of Aveiro.

Blank, L. R. (2013). *international law and Cyber threats.* Newport: Us Naval War College.

Bussolati, N. (2015). *The Rise of Non-State actors in cyberwarfare, in cyberwar: law and ethics for virtual conflicts.* Oxford: Oxford University press.

Friedman, P. S. (2014). *Cybersecurity and Cyberwar what everyone needs to know.* Oxford: Oxford University Press.

Hang, R. (2014). Freedom for Authoritarianism: Patriotic Hackers and Chinese Nationalism. *The Yale Review of International Studies*.

Hang, R. (2017). Cyber-defense Strategies for Contending with Non-state Actors:. *The Yale Review of International Studies*.

Herridge, M. D. (2016, 01 16). *Patriotic hackers' attacking on behalf of Mother Russia,*. Consulté le 02 15, 2022, sur Fox news: shorturl.at/jEFIL

Isnarti, R. (2015). The Role of China's Patriotic Hackers and their relationship to the Governmen. *Andalas Journal for International Studie*.

Johan, S. (2013). *Non State actors in cyber operations.* Stockholm: Swedish National Defence College.

Lokot, T. (2017). *Public Networked Discourses in the Ukraine-Russia Conflict: 'Patriotic Hackers' and Digital Populism,.* Dublin: School of Communications.

Nomaan Merchant, E. T. (2021). *NSA Discloses Hacking Methods It Says Are Used by Russia.* News & World Report.

PRESGRAVES, D. (2021, 12 02). *Unmasking the actors and motivation behind nations state*. (The Corporate Growth…Capital Style blog) Consulté le 02 01, 2022, sur The Corporate Growth…Capital Style blog : shorturl.at/mAKPX

Rens, D. V. (2019). *Patriotic Hackers or Russian Cyberwarfare? Analysing Russian Cyberattacks in Estonia and Georgia.* nternational Public Management and Policy.

Schreier, F. (2015). *On Cyber Warfare.* Washington: DCAF HORIZON WORKING PAPER.

Seattle, C. o. (s.d.). *CEMP.* Seattle: Seattle office of emergency management,.

Segal, A. (2012, 02 12). *The Danger of Patriot Hackers* . Consulté le 01 18, 2022, sur the Diplomat: shorturl.at/bADLR

Studies, T. Y. (2017). Cyber defense Stratedies for contending. *The Yale Review*.

Sunil Kumar, D. A. (2018). Hacking Attacks, Methods, Techniques and Their Protection Measures,. *IJSART*.

Today, Russia. (2017, 06 17). *Patriotic hackers' could exist, but 'Russia does not order state level cyberattacks'*. Consulté le 01 18, 2022, sur Russia Today: shorturl.at/jlHO9

Winterfeld, J. A. (2011). *Cyber Warfare Techniques, Tactics, Tools for Security Practitioners.* New York: Syngress.

Wood, S. (2017). *Patriotic Hacker.* Manchester: A thesis submitted in fulfilment of the requirements of the Manchester Metropolitan University for the degree of Master of Science.