3 CASE-STUDY 2 – THE HACKER COMMUNITY

3 CASE-STUDY 2 – THE HACKER COMMUNITY

3.1 WHITE AND BLACK HAT HACKERS

The 2007 distributed denial-of-service (DDoS) attack against Estonia, the 2008 cyber-attacks against Georgia in the run-up to the Russian invasion, and the use of the Stuxnet worm against Iranian nuclear facilities in 2010 are just a few examples of high-impact cyber-attacks where state support is strongly suspected. The Sony hack and WikiLeaks' NSA-spying revelations are other examples of high impact internet-related crimes that could be interpreted as acts of war in disguise. Despite the fact that these were criminal offenses, some of these actions, notably the Wikileaks revelations, have received some respect from the general public. Hackers are sometimes viewed as "online freedom fighters", exposing injustice and wrongdoing.[97] Stories of hackers who get hired after a successful hack are plentiful.[98] Hacking is hot. More importantly from the point of view of this report, the use of hacker communities represents in many ways novel ways of cooperation that can prove to be successful for state actors.

A hacker can be defined as someone who seeks and exploits weaknesses in computer systems and networks. Some hackers are looking for vulnerabilities to help companies or governments, so called "white hat" hackers.[99] Most hackers, however, use their skills for their own benefit (or just amusement) and no-one else's: so-called "black hat" hackers or, in short, black hats. A black hat hacker who finds a new security vulnerability may sell software exploiting it (an "exploit") to criminal organizations on the black market or use it to compromise computer systems. Black hat hacking occurs in varying degrees of severity: whereas some hackers might be motivated mainly by solving technical challenges or by political or social goals (i.e. "hacktivists") and only involved in relatively minor crimes, others perpetrate serious criminal activities, such as hacking banks to steal money or by paralyzing critical infrastructure. The divide between black and white hats is not always strict: there is also a group of "gray hat" hackers located somewhere between the two. Gray hats do not necessarily work for personal gain, but they might technically commit crimes or perform unethical activities as well.

Whereas white hat hackers are usually employed by computer security companies,[100] black hat hackers will often go to great lengths to remain hidden. They form secret communities and shadow markets. Thus, two forms of cooperation with hackers can be distinguished. First, cooperation within the hacker community itself, or "horizontal cooperation" (see Section 3.1). And second, cooperation between NDOs on the one hand and hackers on the other, or "vertical cooperation" (see Section 3.2). For our purpose, the latter is obviously interesting. But this also applies for the former: knowledge of how hackers cooperate among themselves, how they establish trust, and why they act in the way they do could help NDOs in their own quest for more effective forms of cooperation with more diverse groups of partners.

3.2 COOPERATION BETWEEN HACKERS

In Hollywood, hacking is often portrayed as the activity of a lone individual who attacks major companies from his/her home.[101] In reality, committing serious cybercrimes typically requires cooperation between numerous individuals who often do not know each other and have never met each other in person. This makes searching for potential partners and establishing cooperation in cyberspace a challenging task. Since anonymity is a central part of the online environment, it is difficult to determine who you can trust: putting your trust in the wrong person may lead to being exposed to the authorities.[102]

3.2.1 INCENTIVES FOR HACKERS TO COOPERATE

Incentives to cooperate in cyberspace (versus operating alone) are essentially the same as in other fields of human activity. However, there are some peculiarities that are related to the specific features of the Internet and the illegal nature of, at least, a large part of such cooperation. First of all, working together can increase the benefits (and lower the costs) of a cyber-attack. In some cases, involving more people can increase the direct effect of the attack. This is especially true for DDoS attacks, where scale is essential for success. An example is the 2007 attack on Estonia, which paralyzed the country for three full weeks. Here, a group of Russian activists was furious with the Estonian decision to move a Soviet World War II memorial in Tallinn.[103] Such a large-scale attack is difficult to conduct for a single hacker.[104]

Another strong reason to cooperate is provided by the benefits of specialization. Participants in the underground cyber economy play different roles. Some provide tools for cyber-attacks (exploits, malware, botnets, etc.) or even provide cybercrime as a service. Others offer auxiliary and intermediary services. These include administrators of black markets and mules (who move money or illegal goods from one place to

another).[105] Specialization and the existence of sophisticated black cyber markets lowered the technical barriers to commit cybercrime and as a result expanded the number of people and groups engaged in criminal cyber activity. The same factors also reduce the risk of the final beneficiaries of the crimes being caught because identifying them requires tracing the numerous steps that were involved in a cyber-attack. Easy availability of cybercrime-related tools and services enable a much higher sophistication and complexity of attacks, thus greatly increasing their rewards.

Finally, in case of hacktivism (e.g. Anonymous and some other groups), next to the obvious advantage of scale, hacking together might give the sense of a being part of a group with a mission, or a reassuring feeling of justification.[106] An example is the recent hack on the Ashley Madison website, an online dating site that helps people to cheat on their partner. A group of hackers referring to themselves as 'The Impact Team' hacked the website, stating that the site should go offline or the data of all the customers would be made public. A few days later, when Ashley Madison refused, their data was indeed posted on the Dark Web: 36 million accounts, including names, heights, weights, genders, addresses, email addresses, GPS co-ordinates, credit card transaction details, and sexual preferences were made public. The hackers accused the users of "fraud, deceit and stupidity," telling those affected to "learn your lesson and make amends."[107]

3.2.2 ENSURING QUALITY AND TRUST

The success of the above attacks notwithstanding**,** it is difficult for hackers to trust each other completely due to the anonymous character of the online environment. Most hacking communities reside in what is often referred to as "The Deep Web", where hackers exchange knowledge, skills, and resources through forums and market, and use various tools to remain anonymous. There you can never be sure that the person you are talking to is not simultaneously working for the authorities or will hand you over to the authorities if sufficient proof of illegal activity is collected.[108]

The hacker community takes several steps to ensure a reasonable level of trust and quality of services offered on the black market. One particular system called the "escrow system" was set up in the early 2000s at the CarderPlanet black market. A third party officer was installed, who would mediate between the vendor and purchaser. The vendor, for instance, would offer stolen credit card details that the purchaser was interested in buying. The purchaser would then send the administrative officer a sum of digital money, after which the vendor would sell the stolen credit card details. The officer would then verify whether the stolen credit card worked, and, if so,

would pass the money to the vendor and the credit card details to the purchaser. Through this practice cybercrime in the Dark Web was revolutionized.[109] Fifteen years later, the third-party system is still commonly used in black markets.[110]

Another way is to limit the access to online hacking forums. It is through these forums that hacker groups are usually founded. Most forums can only be entered after a hacker has proven his or her skills, or has been invited by another member – thus limiting the chance of spying by the authorities. Forums often sort their activities on specific topics and practices, such as social media hacking, data theft, malware, exploits, hit-and-run attacks, etc.[111] Examples of hacking forums are EvilZone, HackHound, Bitshacking, Dark0de, and TheRealDeal.

Regular visitors who are active in a certain part of a forum are likely to get acquainted and slowly form a group. This group of friends then might expand by inviting other familiar hackers. Before starting an operation, the group will generally go underground, meeting up in private conversations and closed invite-only channels.[112] This method makes sense, since writing a forum-wide message might compromise the hackers´ operation (spies could inform the target or the authorities, which could solve the security vulnerability, or the actor who posted the message could be arrested). To minimize this risk hackers first organize themselves in a kind of inner circle, looking around forums, checking out who has which skills and who is considered trustworthy, and then inviting those they deem valuable (and reliable) for the new group.

However, sometimes a group that is (still) active in an "open forum", can become a major movement, containing hidden subgroups. An example thereof is Anonymous, which was originally formed in the 4Chan forum where "trolling" activities took place.[113] In 2008, the Anonymous movement started trolling actions against the Church of Scientology.[114] Anonymous launched a DDoS attack on the Scientology websites, combined with real-life actions such as ordering unpaid pizza's and escorts to Scientology churches, faxing images of nude body parts, etc. A short video made by a small group of participants ignited a serious debate within the rank and file of Anonymous. The video declared war on the Church with the result that individuals were spurred into debate and then catapulted onto the streets. Soon, over 7000 people in 127 cities protested the Church of Scientology's human rights abuses and censorships. With this, Anonymous shifted from coordinated trolling to being a political activist group. Over the next two years many joined the Anonymous movement setting up (unrelated) activist subgroups. Participants came to identify themselves as bona fide activists, often performing actions themselves.[115]

The mode of cooperation here is clear. Although Anonymous can be seen as representing a single movement, the structure of the organization is a constantly changing maze where multiple groups organize (and sometimes become quite powerful). Through private conversations and invite-only channels, the overall organization becomes highly complex and confusing. There is no central leadership. No single group or individual can claim legal ownership of the name Anonymous, as it is a classic anti-brand brand, assuming various configurations and meanings. Anonymous is composed of multiple competing groups. This structure makes short-term power achievable for brief durations, but long-term dominance by any single group or person virtually impossible. The sociology of Anonymous is thus a constantly changing labyrinth.[116]

This fluid and opaque organizational structure of many hacking communities also affects the nature of potential cooperation between hackers and NDOs. This kind of vertical cooperation between NDOs and hackers is the focus of the next Section.

3.3 COOPERATION BETWEEN NDOs AND HACKERS

Society's dependence on the smooth functioning of information systems has increased steadily. Cybercrime acts as an uncomfortable disruptor of this reliance. When disruptions to the critical infrastructure caused by a cyber-attack become so severe that they threaten the functioning of the state or, the act may be seen to transcend from the realm of crime into the realm of acts of war. Safeguarding the critical (information) infrastructure then becomes a matter of (national) defense. In trying to prevent or deter – e.g. through the ability to retaliate – these disruptive cybercriminal activities, can NDOs establish cooperation with hackers?

Before elaborating on the possibilities and (potential) benefits and risks of such cooperation, let us first look at some examples of the teaming up of NDOs and hackers in what, depending on the perspective, could be classified as either cybercrime or offensive cyber (as a military act). In its cyber strategy, the Dutch NDO has expressed the requirement for an offensive cyber capability, if anything as a means to retaliate and therefore to deter. In the context of "hybrid" threats and an integrated – equally hybrid – counter strategy, these examples may offer some interesting insights into how NDOs may leverage hacker communities for state purposes.

It should be noted that information on cooperation between NDOs and hackers is limited and, in many cases, classified. This lack of reliable information makes a comprehensive analysis virtually impossible. Yet, research done by computer security

firms, media organizations, and others provide many interesting details about recent high-profile cyber accidents, identifying a number of examples of recent cyber activities where cooperation between various NDOs and hackers is strongly suspected. These examples provide illustrations for a more general discussion of the benefits that NDOs can get by cooperating with hackers, as well as the challenges and risks that they are likely to encounter in the process of such cooperation.

3.3.1 CYBER ATTACK ON GEORGIA

In 2008, shortly before Russia's armed intervention in the Georgian province of South Ossetia, Georgian state computer servers were targeted by a series of cyber-attacks. The attacks against Georgia's Internet infrastructure started nearly a month before the conventional war, with a coordinated major DDoS attack that overloaded and effectively shut down Georgian servers.[117] Although there is no conclusive evidence that the attackers were Russian or acting on state orders, strong suspicions have come up. First of all, security researchers found that the HTTP-based botnet used on the command-and-control server was a MachBot controller, which is a tool that is frequently used by Russian bot herders. Second, the domain involved with the command-and-control server had false registration information but did tie back to Russia because the redirection of Internet traffic went through Russian telecommunications firms.[118] The software programs that controlled the attacks were located in hosting centers controlled by these firms. Some Russian-language websites, such as stopgeorgia.ru, also continued to operate and offer software for download used for DDoS attacks.[119]

However, even if Russian hackers were involved, this does not prove that the attack was also state sponsored. The attacks could be the result of Russia's IT-underground self-mobilization: hacktivists feeling obliged to send out a signal that they were actively participating in the political life and were monitoring events closely. Nationalistic articles in Russian newspapers could fuel tensions further and literally seek involvement of Russian hackers. This could ultimately become a self-fulfilling prophecy: by speculating about non-existent hacker discussions on coordinated attacks against a particular country, such discussions could actually start taking place.[120]

In the example of the cyber-attack against Georgia, it becomes clear that hackers can be an effective tool for instigating DDoS attacks. By mobilizing hackers and hacktivists, one can gain advantages in conventional warfare as DDoS attacks paralyze the opponents' country.

3.3.2 CHINA

In China, the People's Liberation Army (PLA) has also been connected to cyber-attacks on foreign countries. An example here is PLA Unit 61398, a group also known as Advanced Persistent Threat 1 (APT1), Byzantine Candor, or The Comment Group. This last name was derived from the group's trademark of infiltrating computers using hidden webpage computer code known as "comments".[121]

From 2010 until 2012, the group worked each day from nine to five Beijing time, transferring the crown jewels of US corporations' proprietary data out of their networks – and into computers in China.[122] Although Google already reported a hack into their network back in 2010, the group only became publicly known in 2012 after hacking into the e-mails of the president of the European Union Council, Herman van Rompuy.[123] The breach likely enabled the intruders to obtain an insider view into the financial crisis gripping Europe.

However, the hackers themselves were also being hacked. Working together in secret, 30 North American private security researchers (under the leadership of internet security firm Mandiant) exploited a hole in the hackers' security. The researchers created a digital diary, logging the intruders' every move as they crept into networks, shut off anti-virus systems, camouflaged themselves as system administrators, and covered their tracks, making them almost immune to detection by their victims.[124] These minute-by-minute accounts showed a highly organized effort from a group with fixed routines and high success rates. Soon thereafter, the group was linked to the Chinese military, since many of the organizations targeted lost information that could help China in its attempts to become the world's largest economy. The targets included lawyers pursuing trade claims against the country's exporters and an energy company preparing to drill in waters China claims as its own.[125]

The Chinese government denied official involvement, stating that the activity was the work of rogues[126] and that the research would rely only on linking tracked IP-addresses.[127] However, certain parts of the evidence cited by experts suggest that the hacking was in fact state-sponsored. Most convincing was the fact that none of the work was done in the weekend but coincided with Beijing standard working hours. This does not match with the idea of mere hobbyists or hacktivists. Also, the persistence of the attacks was typical for Chinese hackers and the information stolen was mostly about pricing, manufacturing, corporate acquisitions, and contract negotiations.[128]

In this example, another form of cooperation between NDOs and hackers is evident: using hackers through fixed employment. The benefit of this form of cooperation is that it ensures control over hackers' activities and significantly increases coordination of their actions (which in turn increases the success rate). At the same time, the NDOs ability to plausibly deny its involvement, although diminished, remains.

3.3.3 STUXNET

In 2010, a computer worm known as "Stuxnet" targeted industrial and factory systems. Stuxnet was extraordinary – not only because it was, as Alan Bentley, senior international vice president at security firm Lumension has stated, "the most refined piece of malware ever discovered," but also because "mischief or financial reward was not its purpose – it was instead aimed at the heart of critical infrastructure."[129] The Stuxnet worm became famous after it sabotaged the centrifuges used to enrich uranium gas in the Natanz uranium enrichment plant in Iran. Stuxnet was unlike anything ever seen before: it did not hijack computers or steal information from them, but instead destructed the equipment of the controlled computers by placing malicious files on one of the systems. Soon the worm became known as the world's first digital weapon.[130]

Naturally, the question of who was behind the Stuxnet attacks was quickly posed. Security experts who investigated the worm stated that it was almost certainly the work of a national government agency but also warned that it would be near-impossible to identify the culprit.[131] However, strong suspicions have come up that the US and Israeli governments were involved, as they would have had much to gain from a slowdown of Iran's apparent progress towards building an atomic bomb without launching a traditional military attack.[132] According to anonymous US officials speaking to the Washington Post, the worm was indeed developed in cooperation with the Israelis during the administration of George W. Bush. The aim was to sabotage Iran's nuclear program with what would seem to be a long series of unfortunate accidents. The malware was supposed to make the Iranians think that their engineers were incapable of running an enrichment facility.[133] The cyber weapon in this case served clear political motives, namely preventing Iran from acquiring the ability to make nuclear weapons.

The examples described above show the difficulties in determining who was responsible for an attack and whether it was implicitly or explicitly state-backed. Cyberspace is essentially a borderless space where the physical location of an individual does not significantly affect his or her capacity to carry out a cyber-attack.

The internet provides numerous options to hide or to conceal its user's true identity. This makes attribution of a cyber-attack a difficult, and, in some cases, nearly impossible task. Uncertainty and plausible deniability regarding cyber activities make them well suitable for covert operations.

3.4 BENEFITS OF COOPERATION

The examples described in the previous Sections all required at least some degree of either white hat or black hat hacker participation. Cooperation between NDOs and white hat hackers is not a new phenomenon. The Dutch NDO has since late 2013 been actively working on recruiting white hat hackers as so-called "cyber reservists". These hackers are requested to take part in basic military training a few times per year and accompany missions as a cyber security expert, when so required.[134] On top of the reservists program, the Dutch MOD's Cyber Command has, in collaboration with IT security firm Fox-IT, jointly trained defense employees to become cyber security specialists. The first 14 graduates finished their education in May 2015 and were subsequently stationed with the Dutch Cyber Command, the Military Intelligence Service, the Defense Computer Emergency Response Team (DefCERT), and with the Royal Netherlands' Marechaussee.[135]

The novelty factor lies in cooperation with black hat hackers. But why would NDOs consider cooperating with black hat hackers in the first place? One reason could be a superior skillset. Compared to white hat hackers, black hat hackers tend to be more skilled, better trained, and more up to date with the latest security exploits and countermeasures. Black hat hackers will focus only on security penetration and will thus have more security knowledge than other IT professionals.[136] As a result, they are likely better placed to counter other black hat hackers. Therefore, hiring black hatters to test defenses of an organization against cyber-attacks is possibly an attractive idea. Their real world hacking experience is a distinct advantage for security penetration testing.[137] Furthermore, black hat hackers are better equipped to act on the verge, and possibly over the edge, of legality compared to white hat hackers. However, at this stage Western MODs are not, at least not openly, willing to pursue this route.

As Brien Posey, a former gray hat and now white hat hacker and co-owner of a security research firm points out: "There are some things that you just can't learn from a book. (...) Every hack is different because every network is different. (...) Often hackers have to combine multiple techniques or apply techniques in a different way than normal to compensate for various network defenses. Only someone with plenty of real world hacking experience can efficiently go from using one technique to another as required by the present situation".[138]

3.5 RISKS AND CHALLENGES

Successful cooperation between NDOs and hackers is hindered by significant barriers. First, hackers must be identified. Second, they must be convinced to cooperate with a NDO. Third, their work must be coordinated and monitored. Resolving all these problems successfully is not easy. Liberal democracies face additional legal, ethical, and other constraints and barriers in their dealing with hackers. Below we consider these issues in more detail.

3.5.1 IDENTIFICATION

The first problem is to identify hackers with whom a NDO might be interested in cooperating with. As almost any sizeable organization knows, this is not a simple problem even when all conventional recruiting tools (job advertisements, job fairs, recruiting presentations, etc.) are available. These conventional tools can be used in identifying and attracting some hackers, in particular white and gray hats. Hackathons and hacker conferences offer one attractive option for such a recruiting effort. The US government has made notable efforts recruit hackers in this way. In 2011, the US government launched a massive recruiting effort to hire experienced computer employees, who can help defend the nation in cyberspace. To do so, officials from the Department of Defense, the Department of Homeland Security, and the National Security Agency mingled with the 10,000 visitors of DefCon, the world's largest hacker conference.[139] The recruitment effort has been called this generation's "Manhattan Project": the government has set up camps and held cyber competitions for teenagers and has offered scholarships, internships, and jobs in cybersecurity to young adults. With this, the severe shortage of cybersecurity experts working for the federal government should be eased.[140] As the Netherlands also has a shortage of cybersecurity experts, the Dutch NDOs' efforts to recruit cyber reservists and actively train defense employees to become cyber security officials is a logical development.[141] These kinds of efforts are likely to have only limited success in identifying and recruiting skillful black hat hackers. These individuals have strong reasons to hide their real identities and use anonymity that the Deep Web can still provide. So what more can NDOs do to identify black hat hackers? They could choose to infiltrate a hacker community. To do so, a NDO would have to hire an identified hacker and place him or her as a mole in the community. Hiring this one hacker could lead to a snowball effect, as he or she will give away others, who are subsequently incentivized to rat out more hackers to avoid criminal charges. This in turn weakens the entire community structure: it will be difficult for individuals to find each other and forming groups will be particularly cumbersome as there is an increased likelihood that someone in the group is an informer.

Kevin Poulsen, senior editor at *Wired* magazine underlines this view by pointing to the hacker collective's classical vulnerability to infiltration and disruption: "[w]e have already begun to see Anonymous members attack each other and out each other's IP addresses. That's the first step towards being susceptible to the FBI."[142] Conversely, hackers are increasingly aware of this tactic. Barrett Brown, who has acted as a spokesman for the otherwise secretive Anonymous says: "[t]he FBI are always there. They are always watching, always in the chatrooms. You don't know who is an informant and who isn't, and to that extent you are vulnerable."[143]

3.5.2 COOPERATION

After a NDO has identified individuals that it would want to involve in its activities, whether on a regular basis or in an on-call manner, its next step is to persuade those individuals to cooperate. According to Alexander Klimburg, author of "Mobilising Cyber Power", governments have three ways of ensuring a hackers cooperation: coercion, cooption, or convincing.

Coercion assumes involuntary cooperation via the use of negative incentives (sticks), such as pressure, intimidation and force – or threats to use these techniques. Coercion can be used to compel hackers to cooperate who have been caught by offering them reduced sentences or dropping criminal charges against them in exchange for cooperation. This kind of cooperation probably more often takes place as on-call engagements rather than as full time employment. An example here is the case of Hector Xavier Monsegur, or "Sabu" as this celebrated hacker was known online. Monsegur is one of the hacker world's most hated figures, as he turned from being the leading figure in the Anonymous and LulzSec collectives into what was (in effect) an undercover FBI agent. The skilled hacker was facing a maximum sentence of 26 years according to official guidelines but as a reward for having spent much of three years working as a federal informant, was eventually sentenced to time served (equivalent to the seven months he already spent in prison plus one year's supervised release).[144]

According to Eric Corley, a well-known hacker and publisher of the hacker quarterly 2600, Monsegur is not the only US-agent in the hacker community. In an article by the Guardian, he states that one in four US hackers is an FBI-informer, making the US hacker community thoroughly infiltrated. Cyber policing units have successfully forced online criminals to cooperate with investigations by threatening them with long prison sentences. "Owing to the harsh penalties involved and the relative inexperience with the law that many hackers have, they are rather susceptible to intimidation," says Corley.[145]

Russia and China are also likely to use coercion to force cooperation from hackers, but information about such cases does not become public often. In one example from Russia, a suspected cybercriminal appeared in government advisory positions and worked closely with Russian security agencies.[146]

Cooption is another way to promote cooperation with hackers. Cooption is about implied rewards provided through political structures designed to support the political elite. Russia supposedly uses cooption in its cybersecurity strategy. An example here was the Putin-aligned youth group "Nashi", which was implicated in the 2007 cyber-attacks that paralyzed Estonia.[147] Another example is the ATP28 group, which was recently investigated by the cybersecurity company FireEye. According to their report, ATP28's work is sponsored by the Russian government. Not only has the group targeted inside information from governments, militaries, and security organizations that would benefit the Russian government, but the group has also used malware that is developed using Russian language settings during working hours consistent with the time zone of Russia's major cities, including Moscow and St. Petersburg.[148]

In China, cooption is also used by the Chinese government to induce cooperation from hackers. This is, first of all, done through a system called the "National Defense Reserve Forces" program. Through this system, each student enrolled in a technical study automatically becomes part of the Chinese Defense Organization. Furthermore, China's People's Liberation Army (PLA) organizes hacker competitions, through which they identify talented hackers – and subsequently keep them safely occupied. Though the official statement of the Chinese Government is that this cyberwarfare strategy is purely defensive, suspicions have risen that China is operating offensively as well. Governments, companies, and internet security experts around the world have blamed China for many of the past year's global hacking attacks.[149]

The result of China's policy is clear: the country has acquired a strong cyber force, which can – even though China denies it – be deployed both defensively and offensively. However, as Klimburg points out, the bulk of Chinese cyber activity seems to be directed at internal control, either directly (through propaganda, censorship, and collusion) or indirectly (through schemes designed to bind and coopt potentially dangerous individuals, particularly patriot hackers). As with traditional informer systems found in most authoritarian states, the real targets of this system are not the people being spied upon (or, in cyberspace, being attacked). The targets are rather the spies themselves, who are thus coopted by the state and become less likely to turn against the regime.[150]

Convincing is probably the preferred method for a NDO. This means that hackers will voluntarily engage in activities that a NDO would want them to do. In the case of the massive DDoS attacks on Estonia in 2007 and Georgia in 2008 there are reasonable grounds to believe that some participants were motivated by broader national interest (as they saw them) rather than by coercion or cooption. The problem with this particular way of working is that it is fluid and uncertain, and therefore hard to manage. It is difficult to be sure that it can be mobilized at a particular moment in time and at a desired scale.

3.5.3 COORDINATION

Finally, once hackers are identified and convinced, through one way or another, to cooperate, there is the challenge of coordinating and monitoring their cooperation. One particular problem in employing hackers within a NDO is the issue of trust. By definition, black and grey hat hackers would not pass a conventional background check. Can a black hat hacker actually be trusted? How can one be sure that a hacker is not selling a vulnerability he uncovered on the black market, or even worse, inserts a new vulnerability? In other words, how do you make sure that the hired hacker will not become a Trojan Horse? Related to this is the issue that hackers could turn out to be double agents. When the hired hacker finds a vulnerability in a system, he or she could first sell this knowledge on the black market, and only report the leak afterwards. That way, the hacker will receive money twice: once from the seller on the black market and once from the NDO who hired them. Also, in a broader sense, as the hacker will receive knowledge of the systems security, he or she could leak (classified) NDO documents.

In general, taking hackers into your organization is a risky business. Nevertheless, some companies have had successful experiences in hiring black hat hackers. For instance, in 2011 Facebook hired George Hotz, online known as "GeoHot". Hotz unlocked both Apple's iPhone and Sony's PlayStation game consoles and posted details of how to alter software on the devices. This way, crafty tech users could use them for unauthorized games and other applications. Sony, furious with this, publicly sued Hotz on eight claims, including violation of the Digital Millennium Copyright Act, computer fraud, and copyright infringement. After a nasty legal battle of three months, Sony and Hotz reached a settlement. As part of this settlement, Hotz agreed to wipe all PS3 hacking resources from the web. Only a few days after the settlement was made public, Hotz was employed by Facebook, where he was reported to be working on building an anti-hacker defense program.[151] In 2014, Hotz left Facebook to start working for Google, where he joined Google's vulnerability research team Project Zero.[152]

Another example is the case of Nicolas Allegra, pseudonym "Comex", who was hired by Apple in 2011 – only two months after creating the JailbreakMe hacking tools for iPhone and iPad. After one year, Allegra left Apple to start an internship at Google.[153] Allegra was not the first hacker to be hired after successfully hacking iPhones and iPads. In 2009, then 21-year old Australian Ashley Towns created the first known iPhone worm, which set a photo of singer Rick Astley as a mobile wallpaper. Towns was quickly hired by Mogeneration, an iPhone app developer based in Sydney, Australia.[154]

A final example is Michael "Mikeyy" Mooney, who in 2009 (at the age of 17) coded a Twitter worm sending tweets from hundreds of accounts. In an interview with ABC News, Mikeyy said he received several job offers after the attack. The one he accepted was as a developer for Oregon-based web application developer exqSoft Solutions.[155]

In hiring hackers, NDOs should keep in mind that they are not your average employee. Hackers conform to a distinctive subculture, which could result in substantial cultural differences between them and the existing NDO culture. Limiting a hacker's freedom is a general no-go: as soon as a hacker feels restricted, he or she will probably walk away.[156]

Security clearance requirements are likely to be another barrier for hiring hackers. Weed smoking longhairs or hackers with a criminal record cannot possibly obtain the necessary clearances, which limits NDOs in hiring the best hackers out there. To employ truly talented hackers, NDOs will therefore have to broaden the scope of their hiring criteria and focus more precisely on an individual's hacker skills.[157]

3.6 MODELS OF COOPERATION

The problem of how NDOs in liberal democracies could cooperate with hackers is a complex one and involves many legal, ethical, technical, societal, and management issues, which differ from country to country. There are many different ways of organizing and coordinating such cooperation. Applegate proposes four models for incorporating "patriotic hackers" and civilian technicians into militia-like structures and integrating these types of organizations into a state's cyber operations (see Table 4).[158]

MODEL	LEGALLY PART OF NDO?	MEMBER[I]	BENEFITS	DRAWBACKS	COST
FORUM	no	P / A	• Pool of skilled/diverse technicians • No requirements to military standards	• Limited to non-combative activities • Difficult to enforce ethical constraints • Little control • Information leakage	< €
PUBLIC / PRIVATE CELL	no (in most cases)	P	• Higher security level • Difficult to infiltrate • Flexible in duration • Specific skillsets	• Traditional contracting practices • Vetting required	€
REGULAR RESERVE	yes	P	• Well trained experts • Formal induction into military • Fast mobilization	• Active duty standards • Little incentive for formal induction • Formal training requirements	€ € €
CYBER READY RESERVE	yes	ex-P	• Highly qualified technical professionals • Quick mobilization • Legal combatant status • Traditional ethical, legal, and operational constraints • No formal training	• Difficulty of organizational integration • Little understanding of the mission • Difficult to match experts and place • Little skill validation or maintenance	€ €

TABLE 4: FOUR MODELS FOR DEFENSE-HACKER COOPERATION. SOURCE: APPLEGATE, 2012.

P= PROFESSIONAL. A= AMATEUR.[159]

The first of Applegate's models – the forum – uses formalized forums for limited cyber operations. The membership is primarily composed of security professionals, security researchers, and technicians. States could use these forums for open source research, code review, and as a recruiting pool for selected projects. While inexpensiveness and no requirements of military standards on appearance or physical fitness make this model lucrative, it is also difficult to enforce ethical constraints or control actions of

individual forum members. More importantly, there is a risk of information leakage: it would be easy for a competitor state to infiltrate this type of organization.[160] An example of a forum model is the network of Warning, Advice and Reporting Points (WARPs) in the UK. A WARP is a forum of 20 to 100 members created to provide warnings about possible cyber incidents to its members – either local governments, legal organizations, or businesses. At the head of a WARP, there is an operator who distributes the information among the members.[161]

The public/private cell model puts together a small group of hackers who most likely know each other in a group or cell. This composition is more secure, more difficult to infiltrate and would also make use of members´ specific skill sets. On the other hand, traditional contracting practices would probably be required, and members' background would also need to be examined.[162] Two examples of hacker cells are "Team Evil" and "Team Hell", even though these are not known to have cooperated with defense.[163] Team Evil, an anti-Israeli hacker group, was predominantly active in 2006 when it attacked over 8,000 websites of Israel and other countries, such as Saudi Arabia, China, and Indonesia. Team Hell is a secular Saudi hacker group which has shown aversion to the Israeli and Syrian regimes and al-Nusra, for instance.[164]

Applegate proposes two other models for cooperation between NDOs and civil technicians or ICT experts – the regular reserves model and the cyber ready reserves model. The former encompasses employing active duty military personnel in cyber operations and the latter recruits "cyber soldiers" – professional soldiers that have finished their military service obligation.[165] These models essentially focus on building cyber security capabilities within NDOs through education and training. Neither model, however, directly touches upon the nature of the cooperation between the defense forces and hackers and as such are not discussed in more detail here.

3.7 APPLICABILITY FOR NDOs

It is evident that cyber space is becoming more and more important for NDOs. Both defensive and offensive cyber capabilities need to be strengthened. The use of skilled hackers might well form part of this capability build-up. Hackers have better knowledge and skills of how to gain entry into a system then classically educated and operating IT professionals, since they have real world hacking experience. On the downside, we see two principal disadvantages or risks in employing hackers as part of the cyber capabilities of NDOs:

- *Trust*: it remains difficult to know whether a hacker is truly working for you. Because of their unique skills and the difficulty to monitor their work, hackers might become double agents, revealing critical vulnerabilities to criminal organizations or other countries.
- *Culture*: there are fundamental differences between the hacker culture and the typical military culture that may create severe tensions.

In working with hackers, there is a crucial difference between so-called white hats and black hats. In many respects, employing or hiring white hat hackers seems not very different from engaging other types of specialists. There might be an issue of whether governments can afford to employ the capable ones, but that is no different than, say, for other scarce categories. This is a route already taken by the Dutch MOD. It is too early of a stage to assess whether it is a successful route, but it seems likely that any obstacles along the way would rather point toward other solutions to negotiate the route instead of choosing to abandon it altogether.

Engaging with black hat hackers is a completely different story. It would be a principled choice to engage with black hats at all, considering the political, judicial, and ethical liabilities. For manty western NDOs, the will and authorization to do so in a structural way seems unlikely. And even then, a host of practical questions and difficulties arise. These principal and practical issues must be set against the anticipated benefits. Reasons for using black hats may, for instance, be that they are better skilled, more versatile, and more up to date with the latest security exploits than white hats; have a much wider range of options beyond what government agencies may do; and that they are better placed to counter other black hats (it takes a thief to catch a thief). In our (limited) analysis, apart from some anecdotal snippets, we have not been able to come up with conclusive facts and figures to either substantiate or dismiss these propositions.

An intermediate solution would be to employ black hats turned white. However, it might be that many of the potential advantages of using black hat hackers quickly disappear once they are brought within the operational and legal framework associated with white hat hacker activities.

There is, however, another angle for taking a closer look at how hacker communities operate from a NDOs' perspective. The hacker community operates on, and often beyond, the brink of legality. In the twilight zone of the dark web, relationships are

forged. Because of their clandestine nature, these relationships are either very exclusive or fleeting, often lacking a basis of trust, and therefore as a rule uneasy, if occasionally very rewarding for the participants. In contrast, NDOs typically enter into long-term relationships with trusted partners, based on formal agreements and well-understood, stable mutual interests. However, there is a distinct trend for NDOs to engage not only in long-standing, high-trust partnerships, but also in more ad hoc, informal, and even implicit forms of cooperation with unfamiliar parties, and even with parties considered untrustworthy or outright hostile. The complexity of the security environment increasingly demands willy-nilly interactions with actors one would rather not engage with, but that within a given situation may be instrumental in achieving certain desired political or strategic effects. Some of these interactions may indeed resemble the way in which hackers engage one another. It is this realization that makes this case interesting: what may NDOs learn from methods the hacker community employs to create goal-oriented working relationships between agents that do not really know each other, do not trust each other (or even actively distrust one another), and might even have contradicting values and interests outside the scope of a limited and temporary alignment?

Within the scope of this study, we did not elaborate much on this particular angle. But it certainly seems an interesting notion to pursue further elsewhere.

3.8 PRACTICAL EXAMPLES

China and Russia can more readily coerce, coopt, and convince hackers than most Western democracies – although a large portion of their cyber activity is directed at internal control rather than on external use.

One of the more recent cases where Russia's offensive cyber power became apparent is in Ukraine. Ukraine has been faced with a separatist conflict in its east for two years now, during which the Russian government has been suspected of instigating numerous cyber-attacks. For instance, BlackEnergy, a Russian malware, was used in the summer of 2014 against the Ukrainian government by a hacker group called Quedagh.[166] In October of that same year hackers, most probably Russian, attacked several computers of international organizations, companies (for example energy companies), and the Ukrainian government. The attacks are believed to be part of a years-long operation of Russian hackers due to the code language and the targets involved.[167] In late February and early March 2014, telecommunication company Ukrtelecom came under attack. The vast majority of regional services provided in Crimea were soon out of order.[168] The attack also influenced the mobile phones of

Ukrainian politicians, which were blocked by malicious software.[169] While it is not confirmed who was behind the attack, it is believed that the unknown hacker or group of hackers were affiliated with the Russian government, with the aim of isolating Crimea from Ukraine. It is suspected that the Russian vessels that arrived in Sevastopol contained jamming tools and hence were placed there in order to hinder radio transmission.[170] Around the same time, other Ukrainian actors faced cyber-attacks, such as the UNIAN news agency and the journals Glavnoe and Gordon. The Ukrainian government, Verkhovna Rada, and the Ukrainian Security Service also faced DDoS attacks.[171]

China's use of offensive cyber capabilities is illustrated by the example of one man, Tan Dalin, which is described in a document posted by the Obama Administration.[172] As a student, Dalin was invited to participate in a People's Liberation Army (PLA)-sponsored hacking contest. When he won, he formed the group "Network Crack Program Hacker" (NCPH) and recruited other talented hackers from his school. He managed to find a funding source (unknown benefactor) and started attacking US sites. After an initial round of successful attacks, his funding was tripled. Throughout 2006, NCPH built sophisticated rootkits and launched a barrage of attacks against multiple US government agencies. By late July 2006, NCPH had created around 35 different attack variants for one MS Office vulnerability. During the testing phase, NCPH used Word document vulnerabilities. Later, they switched to Excel and PowerPoint vulnerabilities. The result of all of this activity is that the NCPH group siphoned thousands, if not millions, of unclassified US government documents back to China.[173]

What these groups consist of and how they work is mentioned in Kathrin Hille's work "Chinese Military Mobilises Cybermilitias": "[These groups comprise] 25-year-olds or 17-year-olds [who] have 40-year-old fathers who happen to be working within institutions. Very often the opportunistic exploitation of a particular low-tech approach is derived through that chain, completely informally, rather than through somebody sitting in committee and deciding let's build 500 botnets that we're going to use to attack the Tibetan community."[174]

It is not a given that Western NDOs can go down similar routes. The problem of how NDOs in liberal democracies should cooperate with hackers is a complex one and involves many legal, ethical, technical, societal and management issues, which differ from country to country. Applegate proposes four models for incorporating patriotic hackers and civilian technicians into militia-like structures and integrating these types

of organizations into a state's cyber operations (see Table 5). Two of these four models are non-traditional in nature. The forum model uses formalized forums for limited cyber operations. The membership is primarily composed of security professionals, security researchers, and technicians. States could use these forums for open source research, code review, and as a recruiting pool for selected projects. While inexpensiveness and no requirements of military standards on appearance or physical fitness make this model lucrative, it is also difficult to enforce ethical constraints or control actions of individual forum members. More importantly, there is a risk of information leakage: it would be easy for a competitor state to infiltrate this type of organization.[175] An example of a forum model is the network of Warning, Advice and Reporting Points (WARPs) in the UK. A WARP is a forum of 20 to 100 members created to provide warning about possible cyber incidents to its members – either local governments, legal organizations, or businesses. At the head of a WARP, there is an operator who distributes the information among the members.[176]

The second non-traditional model is the public/private cell model, which puts together a small group of hackers who most likely know each other in a group or cell. This composition is more secure, more difficult to infiltrate and would also make use of members´ specific skill sets. On the other hand, traditional contracting practices would probably be required, and members' background would also need to be examined.[177] Two examples of hacker cells are Team Evil and Team Hell, even though these are not known to have cooperated with defense.[178] Team Evil, an anti-Israeli hacker group, was predominantly active in 2006 when it attacked over 8,000 websites of Israel and other countries, such as Saudi Arabia, China, and Indonesia. Team Hell is a secular Saudi hacker group which has shown aversion to the Israeli and Syrian regimes and al-Nusra, for instance.[179]