Chapter 2

The hacker group

R. Gevers

CHAPTER OUTLINE

INTRODUCTION

Since the information revolution the Internet has been a driving force behind many—if not most—social reforms. From the 1% marches to the Arab Spring: The Internet was used to fuel, coordinate, and facilitate protests. The Internet turned out to be a safe haven for liberal thinkers and was used to establish contacts with other like-minded individuals at the other end of the globe. The global nature of the Internet makes (targeted) communication accessible to anyone. This was at the core of many great revelations: WikiLeaks being the first, The Intercept and Edward Snowden following quickly.

In the early days the Internet was a safe haven for free thinkers; there was no censorship and no laws were directly applicable. This opened up opportunities on the Internet to influence governments and their laws. However, this situation has changed: The Internet has become securitized and militarized. Whereas the Internet used to be a place aimed at free and unhindered flow of information and ideas, now it is increasingly influenced by State actors and large non-State actors. Whereas any individual could tread onto the Internet and fight for a cause, nowadays you need to tread carefully.

Chapter 1 has described the essence of cyber guerilla strategy, tactics, and the concepts of favorable and unfavorable terrain. In other words, Chapter 1 has laid out the overarching conceptual framework for cyber guerilla. As mentioned in Chapter 1, cyber guerilla is amorphous; it takes different forms depending on societal context. It may take a nonviolent form, resembling electronic civil disobedience, or a more violent, conventional guerilla-like form, albeit virtual.

These different contexts require a versatile, intelligent, and very specific type of individual to fight on the digital forefront. This chapter will zoom in to look at the cornerstone of cyber guerilla: the hacker group. Sections 1 and 2 will focus on the two roles hacker group members have to be able to fulfill. Mirroring the amorphous character of cyber guerilla, group members should be able to fulfill the role of (1) social reformer and (2) combatant. These two sections are aimed at describing the ideological foundations of hacker group members. Section 3 describes the hacker group composition and will describe the intellectual capacities and skill-sets needed in the group.

THE HACKER AS SOCIAL REFORMER

Anyone wishing to make a stand against a larger actor will ask himself what type of persons are sought after when organizing a hacker group. The type of person sought after can best be described as a social reformer, strongly developed in both intellectual and ideological sense. This person shares the firm belief that traditional laws do not apply to the Internet and the borders that sovereign rulers try to impose on the Internet are irrelevant. Although most political leaders will try to bring their laws onto the Internet, he believes that they will not succeed, in part because of his contribution to preventing them from doing so. He believes in the Internet as common good enabling the connection of communities and sharing information, knowledge, and ideas.

It should be stated that the Internet has enabled a borderless guerilla fighter. The territory of the cyber guerilla fighter is the borderless Internet. The Internet is the connecting element for fighters located in different territories. As a consequence of the global character of the Internet, new recruits can be found anywhere on the planet. This global character is reflected in the cyber guerilla fighter—he is a human being but, unlike many others, he does not feel bound by borders. Believing in a free, unhindered flow of information and ideas, he is not interested in religion, ethnicity, and sexuality. Information, knowledge, and technology prevail over any these irrelevant aspects.

The Internet functions as brains and nerve system for the hacker group. The Internet enables the hacker group to tap into a vast resource of community knowledge (brains) and to direct action via myriads of channels (nerve system). As Internet access permeates the world, the potential recruiting ground increases and offers many more to join the fight against all forms of injustice. Cyber guerilla is not an exclusively Western phenomenon; as the domain is global, possible recruits can hail from anywhere. As Internet access is benefiting cyber guerilla, the guerilla fighter should always strive to enable Internet access to those being cut off, censored, or otherwise unable of reaching the Internet. Giving or restoring people's access will increase the amount of potential recruits and supporters.

The individual sought after strongly opposes Internet censorship and feels he should fight against this form of oppression. Although the battle for a free Internet has been long lost, there are many new opportunities to escape, evade, and counteract the scrutinous eyes of States, large corporations, and other actors. These means open to any individual will be discussed later on in this chapter and Chapter 3. Besides that, the individual fighting cyber guerilla believes that only the Internet can guard our freedom of conscience, which is the only thing that could further humanity technologically, culturally, and sociologically. This individual is not trying to achieve megalomaniac feats as saving the planet; instead he aims to improve the quality of life for all gradually.

THE HACKER AS COMBATANT

As States and large actors seized the information domain, they sought ways of influencing other actors. The hacker and his code turned out to be a very effective weapon on this virtual battleground. In the beginning of the Internet, monitoring was virtually nonexistent; hence, anyone with a little hacker skill could penetrate any of its chosen targets. Without getting caught, one could easily wander through the computers of NASA or visit AREA51 digitally. The many videos of old-school hackers penetrating army.mil server, filming it, and throwing it online are testament to this period in time where anybody could hack. Sadly enough, by virtue of intrusion detection systems going mainstream that age is over right now. To overcome access controls and all other safeguards, a very knowledgeable and skillful individual is needed.

These types of individuals are very scarce and are sought after by IT companies, armed forces, intelligence agencies, and large corporations. As anyone is looking after these individuals, knowledge and skill have become the prime criteria above all else. For once soldiers do not care about the

hacker's physique, as long as they are capable of shutting down the enemy's air defense system. The hacker in a combatant role has proven to be very effective, able of influencing large corporations and States.

Stuxnet is one of the most prominent examples of the potency of hackers in State-to-State relations. Government-funded hackers created Stuxnet and released it to manipulate the Natanz centrifuge. Although heralding the state and its intelligence agencies as the victor, this success was achieved only by virtue of hackers. Another example affirming the role of the hacker on the world stage is Edward Snowden's revelations. The Snowden files uncovered a virtual arms race in the realm of digital and economic espionage. The means and methods used in this arms race are developed, maintained, and executed by hackers. These examples affirm the power of the Internet and information technologies, and the role of hackers on the world stage.

Not only do hackers play a potent role in the arena of State-to-State relations; they are a force to be reckoned with even in internal affairs. As the Arab Spring and many other smaller protests have shown, one of the most successful ways of spreading ideas is through social media. Many governments try to censor such platforms and try to impose controls on these platforms. Censorship and controls are easily overcome by hackers; they can help movements by training and educating the protesters in ways of circumventing censorship. Although no hacker is needed to start a movement, hackers can make sure that governments will not succeed in tampering with movements, impeding on their outreach and their effectiveness in general. Examples include overcoming domain name system (DNS) censorship in Turkey, the Arab Spring (Tunisia, among others), and censoring BlackBerry usage during London riots. As such, hacker skills contribute to movement success. Exponential growth has gotten a new dimension with the rise of the Internet and social media—the hacker is the maintenance engineer and champion.

In the past decade we have witnessed many hacker groups operating—whether in support of or against a State actor—from conflict zones. Conducting operations from areas that are subjected to armed violence requires a different mind-set and organization. When conducting cyber guerilla during armed struggles, whether inter- or intra-State, the hacker group has to be prepared for physical violence, detainment, prosecution, and abductions. Hacker group organization capabilities, and the different tasks should be prepared with the utmost care when preparing for operations during conflict. Hacker group leadership should play a prominent role to prepare the group for this daunting challenge.

Acting against State or non-State military or militant actors involves the hacker group becoming a potential target for these actors. These actors have shown the willingness to use deadly force against those engaged in cyber activities, for instance by bombing their homes and workplaces. Other activities are the detainment or abduction of members by State agents, all showing that military or militant actors will most likely choose to counter hacker operations with physical force rather than virtually. The hacker group should prepare for this contingency when taking on a role in armed conflict.

Some might feel that the hacker group will not be targeted by physical action. The following example will illustrate what a group might expect when conducting activities during armed struggles.[1] The means and methods militant or military actors will use against (hacker) groups become apparent when looking at the group "Raqqa is Being Slaughtered Silently" (or Raqqa_SL) in Syria. This group is spearheading the Syrian media campaign against Islamic State (IS) in Raqqa. This group primarily focused on the use of (social)media to unveil the monstrosities committed by IS. This particular group is conducting extremely difficult work in an extremely hostile environment. Several of its members have been killed, not only within the occupied area in Raqqa, but also in other countries (such as Turkey). This exemplifies that a virtual activity may result in physical repercussions; a group that is conducting operations or something as simple as providing media coverage for the world to see have the risk of being killed.

The mind-set required is being prepared physically and morally for counterattacks by the opponent, not only virtual, but also physical attacks. When the hacker group is conducting operations that are hurting the opponent, the opponent will not shy away from drastic measures against the hacker group.

THE HACKER GROUP

The hacker group is the core of cyber guerilla and every operation undertaken. This section will describe the hacker group and its composition. The hacker group as a whole can exist out of numerous individual groups, but all should share the same goals. Operating as a whole of numerous individual groups should be, as mentioned in Chapter 1, a conscious choice of the leadership within a hacker group and depends on societal context, the opponent, and the state of the hacker group. To align the goals over different groups, a clear goal and strategy for achieving that goal should be formulated in the beginning stages of the hacker group. Whether there

[1]The authors are indebted to Guido Blaauw for writing this section on mindset required during conflict.

are multiple small groups or one large group, there are general tasks within hacker groups which should be taken care of. To be an effective hacker group, it is very important to specifically assign tasks to all individuals within the hacker group.

Disciplines

There is a variety of specific tasks within the hacker group; all of these tasks should be practiced with full dedication. Only in very specific cases can tasks be ignored as they are temporarily less relevant—for instance, the external communication discipline when establishing initial compromise. However, in most cases all of these disciplines should be fulfilled for the hacker group to succeed. The following sections will describe the different disciplines within a hacker group: leadership, infrastructure, internal communication, recruiting, engineering, forensics, command and control, development, and external communication.

Leadership

The core of the main hacker group should ideally consist of six individuals with one natural leader, but this is not a requirement and depends on the context of the operation. This nucleus is the leadership within a hacker group. The leader should be the one that spends most time online, is dominant by nature, but most importantly is able to understand all technical aspects of an operation. The leader of the hacker group should be verbally strong and possess strong technical skills.

The hacker group and its members are very vulnerable to egoism; members may decide to engage in operations for their own gain instead of trying to achieve the goal of the hacker group. Hackers are very vulnerable to getting caught up in their love for using and exploiting technology. To counteract this drive during an operation, the leadership should always keep the goal in mind and never let members of the group do anything else than their previously determined task. Becoming domain admin might be rewarding, but it is not always the goal of the operation and may result in unwanted attention. Conducting these types of unplanned tasks could compromise the whole operation and endanger all members engaged in the operations.

Besides keeping track of the hacker group's goals and progress in achieving these, leadership should also be vigilant of potential leaks within the hacker group (moles or snitches). In some cases hacker group members may be recruited by an opposing actor (law enforcement, other hacker groups, criminal organizations). The leadership should evaluate the loyalty of all members of the hacker group on a continuous basis. To prevent the leadership

from being corrupted, one should not be able to easily join the core of the hacker group.

There are several guidelines with regard to the leadership structure within a hacker group. The pivotal points in the leadership structure revolve around 6 and 12 members An ideal group consists of 6 core members; whenever this group becomes more than 12 members the leadership structure has to be reconsidered and restructured. When considering restructuring it is best to apply a layered structure. Every layer should have its own degree of security and trust. The top layer, the six core members, should have the most stringent controls, safeguards, and precautionary measures in place. Should the group grow even further, new levels can be added to incorporate new members; these new members should be added to the bottom peripheries of the organization. Come time and once proven to be trustworthy, they can gradually climb within the organization.

Infrastructure

Another distinct set of tasks within the hacker group is infrastructure acquisition and maintenance. The ideal choice of infrastructure differs per operation; those responsible for planning and conducting operations should determine which type is suitable. There are many options with regard to infrastructure, all with specific advantages and risks. These aspects should be carefully assessed and evaluated in choosing specific infrastructure. Aspects to be taken into account are, among others, reliability, uptime, bandwidth, and interception possibilities. The following sections will describe different types of infrastructure and their advantages and risks. Note that this infrastructure is the attack platform for the hacker group but can also be used for communication and anonymity.

Hacked infrastructure

Hacked infrastructure is the infrastructure available to a hacker group as a result of obtaining control over infrastructure via hacking. The main benefit of using hacked infrastructure is that it is free. If the hacker group lacks sufficient funding, using hacked infrastructure can be an outcome. Using hacked infrastructure also has many downsides. The hacked computers will go down very quickly; often hacked server do not last longer than a maximum of 2 months. It is essential to know different types of infrastructure which can be hacked; the following sections will describe virtual private servers (VPS), dedicated servers, and shared web-hosting servers.

Shared web server. Shared web-hosting servers are the least beneficial. They are very easy to hack, but as it is easy to hack a shared web-hosting server, the hacker group is often not the only one hacking the server. Apart

from the weak access controls, shared web hosting often has bandwidth limits in place; running out of bandwidth will result in the website going down. The bandwidth of a shared hosting web server is often low; hence they offer a very limited advantage to a hacker group. Another downside is the tendency of shared web servers to notify the owner of a website when the website runs out of resources; this could compromise ongoing operations of the hacker group. Apart from weak access controls and notifications to the owner, another downside of shared web servers is that some are maintained almost daily by system administrators. This means dedicated system administrators login on a daily basis to perform actions on the servers (eg, upload content, inspect logs, monitor bandwidth, look at analytics, etc.). These system administrators can be assumed capable of spotting hackers. This, again, could compromise the operation and cause unwanted attention.

Virtual private server. VPSs can be very useful as they often have good bandwidth and are not maintained on a daily basis. The problem here is the fact that VPSs often still have bandwidth limits. Once the server runs out of bandwidth, corrupting the operation, the owner of the website may be alerted. This could result in the hacker group's operation being compromised. Apart from running out of resources, the owner may also be alerted by the monthly bill, which may show extensive usage of the VPS.

Dedicated servers. Hacking a dedicated server can be very useful for the hacker group. Those are often the servers that perform just one task, have a default installation, and are not maintained on a daily basis. They usually have a big Internet connection because they are very important to the company owning them.

Higher bills at the end of the month because of increased bandwidth usage are often ignored and the bills are paid by the company because the server is that important to the company. If the hacker group decides to use a dedicated server as their main platform for reliable communication, it is recommended to run the server first for a few months and only after a few months decide upon switching. The first few months are the critical phase; if this server turns out to be stable during that time it will often stay online for a very long period of time.

Physical access infrastructure. Physical access infrastructure is the type of infrastructure which can only be used by physically moving to its location: for instance, war driving or accessing the network infrastructure at a McDonald's restaurant. This kind of infrastructure is not recommended. The infrastructure by itself is often unreliable, slow, monitored, and often heavily fire walled, let alone the possibility of surveillance cameras in the neighborhood capturing your presence. These networks can be useful though

when very specific operations are going to be executed. This type of Internet access can be considered an extra layer of defense as it is geographically separated from the rest of the infrastructure of the hacker group. Some might ponder using the (wireless) network of neighbors. Using wireless Internet in the vicinity of a member's private residence is not recommended. Neighbors and other locals often know that someone is technologically proficient; any event relating to covert Internet activities will result in suspicion.

Infrastructure ordered with stolen credit cards

Infrastructure bought with stolen credit cards can be very useful. It provides the hacker group with the ability to use reliable infrastructure at a location of the buyer's choosing. Besides choice of location, buying a server will also make sure that the hacker group can select the server with the right disk space, processing capacity, bandwidth, management, and maintenance.

This type of infrastructure is ideal for a hacker group, for instance, if a hacker group would require a server to store large quantities of data extracted from a company as quickly as possible. One can choose a geographical location close to the hacked target and make sure the latency to the hacker target is as low as possible, making sure as much data as possible can be exfiltrated from the company in the least amount of time. Once the data are exfiltrated and put on this server it can be further spread to safer locations. After the need for the server is gone the server can be dismantled. Discovery of stolen credit card credentials is always imminent; this is the downside of purchasing infrastructure by using stolen cards. Eventually the credit card company will find out and revoke the credentials—this will most likely result in the hacker group's server shutting down. Luckily investigations into credit card misuse are rare; it is paramount, however, to be aware that the these types of activities can alert opponents and supporting actors.

Anonymously purchased infrastructure

Purchasing infrastructure anonymously is most ideal for creating long-term infrastructure (several years or more). Payments should be made anonymously, for instance through digital currencies relying on blockchain technology and prepaid credit cards. The hacker group should make sure that anonymous registration information is provided. Besides that, the hacker group should tread carefully in using the server, for instance the hacker group members should never login to any administration panel of the server from one's home server. This mistake is often made, that is, there are known cases of people contacting the hosting provider's helpdesk and signing off with their real name. This will result in operational comprise and severely impede the hacker group's operations.

Other assets

Apart from attack and communication infrastructure, there are other assets which might be obtained that are beneficial to the hacker group. The following section will list some of these assets and briefly describe their purpose and how to obtain them.

Code signing certificates. Code signing is a technique used mainly by the Windows operating system since their Vista version. The purpose of code signing is to detect whether someone is trying to illicitly tamper with the operating system. Before one can manipulate a Windows system driver, for example, the driver has to be signed. If an unsigned driver is used, several security precautions will be triggered. Therefore, it is recommended for the hacker group to be in possession of several code signing certificates.

Although people tend to think the process of obtaining a code signing certificate is difficult, in reality it is not. Developers tend to upload all their projects and code snippets to cloud storage solutions. As a consequence of the wide and careless use of these code signing certificates, there are a lot littered around the Web. Certificates can be found on Github, Pastebin, peer-to-peer networks, and online open directories. It is recommended for the hacker group to gather multiple certificates; they can obtain these from the aforementioned media.

Another way to get possession of certificates is to manipulate the certificate system; one can easily register fake companies and find online copies of identification documents that can be used to buy a code signing certificate. Buying your own code signing certificate gives the hacker group great control over the certificate itself, whereas using a stolen certificate offers fewer options and is primarily useful as an Easter egg. Which method of obtaining a code signing certificate is most beneficial to the hacker group depends on their operation.

VoIP servers. Voice over IP (VoIP) servers can be a great asset to a hacker group. Access to a VoIP server can help the hacker group to gain intelligence and to enable making VoIP calls under the guise of the company owning the VoIP server. Voice is still considered to be a very personal and direct way of communicating; trust is more easily established once a person's voice can be heard. As such, phone calls are still frequently used for social engineering activities. The hacker group can use VoIP servers for social engineering purposes but also to listen in on conversations taking place between employees (intelligence).

Obtaining VoIP servers can be very easy since there is an increasing amount of these servers around and many of those servers are improperly administered. Many of these servers are configured wrong, resulting in "open"

servers, or not configured at all, resulting in "default" setting. Vulnerable VoIP servers are often listed on online vulnerability, exploit, and scan databases such as ShodanHQ. The hacker group could usurp the vulnerable servers, for instance, to listen in on conversations, use in social engineering, or internal and external communication.

Internal communication

An important task within the hacker group is providing communication for the hacker group itself. One or more members should be tasked to provide infrastructure and software to make communication easy and user-friendly. The infrastructure used to communicate must be run on dedicated hardware (see the section on infrastructure). This means that the infrastructure chosen to run the communication platform must be in full control of the hacker group and be completely trusted. Communication platforms are very vulnerable to wiretapping; hence, all communication within a hacker group should be encrypted.

The hacker group should further enforce strict procedures for accessing and using communication platforms. The hacker group should always keep in mind that every `ACK` packet sent—whether an `RST` or `ACK`,`SYN`—is registered and thus contains compromising information. Hence, when a hacker group chooses to use servers as their main communication channel, these should be made accessible only through The Onion Ring (TOR) network. This way the hacker group can guarantee that members, trainees, and other persons requiring access do not connect from their home addresses. Although taking precautionary measures, the hacker group should always be vigilant and never forget that servers are the most viable and useful for opponents and law enforcement agencies to tap. Therefore, the hacker group should make sure that everyone connecting to these devices is disciplined always to use encrypted communication channels.

The main communication platforms for hacker groups are TOR network, Internet Relay Chat (IRC), forums, and mobile messaging. The following sections will discuss certain elements to keep in mind when creating, maintaining, and administering these platforms.

The Onion Ring network

TOR network is the only network recommended for use by the hacker group. While initial communication and simple information gathering can be done without TOR, once operations are coming closer the hacker group should always switch wholly to communication over the TOR network. The reason for doing so is that the TOR network is the only network protecting your

true physical location on the Internet. Besides that, it also offers safeguards against wiretapping. Apart from using the TOR network, the hacker group should always use other layer(s) of encryption to communicate, for instance run plain text through another cryptographic tool before sending it via the already encrypted communication channel.

Many hackers using TOR generally make one huge mistake: they install their TOR client on the same computer they perform operations with. This will result in unprotected network traffic when TOR client crashes or unexpectedly terminates. After crashing or termination, the running tool sets to search for a new connection; it will find one over the regular Internet connection. Another related problem could be data leakage due to wrongly configured programs that bypass the TOR network and set up their own connection, resulting in personally identifiable information leaks. Once this has happened log files at the target site can be used to determine the attacker and compromise their identity. This could cause operational failure and have severe repercussions for the safety of the hacker group.

The hacker group members should share best practices regarding optimal use of the TOR network and precautionary measures. It is essentially up to the hacker, however, to take appropriate measures to prevent Internet access if the TOR Internet connection goes down. This can be achieved in several ways. One of them is putting a tunneling device (for instance, a bridge or other dual-interfaced device) between the device that is being used to access Internet resources and the outward-facing Internet connection. Using this method, hacker group members can make sure all Internet traffic is routed onto the TOR network. Devices such as the Raspberry Pi can be used for this purpose; they are cheap ($80) and offer great value for the money.

Internet Relay Chat

Communication within the hacker group is often performed through IRC. Hackers tend to favor IRC as it is close to command line and easily scriptable. Another reason hackers favor IRC is that it does not have specific disadvantages. As previously mentioned, the infrastructure to host the IRC channels on must be trusted. That being said, the hacker group should operate on the notion that the channel will be wiretapped. To thwart attempts to listen in on conversations, IRC provides many ways to encrypt its communication. It is up to the hacker group to enforce a strict policy of mandatory channel encryption. Preferably all channels should use its own scheme of encryption; there should never be a standardized predictable encryption scheme or reusage of passwords.

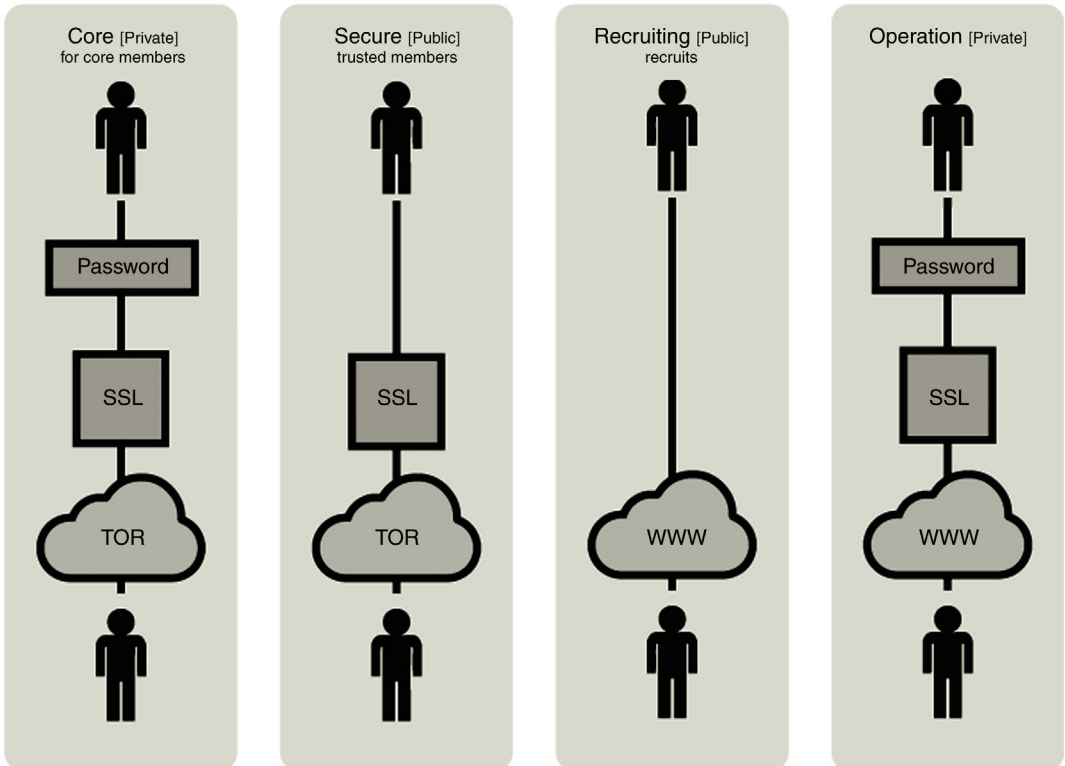
Wherever an ongoing campaign is coming to a climax the hacker group should always switch to a temporary server and channel. The hacker group member tasked with communication should facilitate this infrastructure and take care of its reliability and encryption. Not until the last moment should location and encryption details be communicated with all individuals joining the operation. Only when all members taking part in the operations have joined the channel should detailed information regarding the operation be communicated. Once the operation has been successful the server and channel should be left immediately. Details regarding the channel should be stored on a server that only a select number of individuals can access.

It is up to the hacker group to enforce a strict IRC channel policy—one of the elements needing discipline is posting links. This should be prohibited on both IRC and forum communication platforms since the chances of anyone accidentally revealing their identity by clicking on a (malicious) outbound link is too large. Although everyone knows not to click links and to mask their IP address, an individual of the group will click that link and will reveal its identity. Once the identity of one member of the hacker group is compromised, all hacker group members are in great danger. Therefore, links should always be forbidden and removed. Links can be replaced by a simple "hxxp" or "redacted," as long as they are never interpreted by any interpreter as existing links. The hacker group members should always educate and train each other on how to properly and consistently make use of technology to mask their true location on the Internet. Apart from that, hacker group members and leadership should also train and force members to change their online identities frequently. The use of digital sock puppets clouds the activities undertaken by members; not taking these precautionary measures may result in the member being profiled.

Apart from forum and IRC policy, the forums need to be built in such a way that they only allow TOR exit nodes to connect. Again, note that this does not result in perfect safety, as failing Transmission Control Protocol (TCP) connections will still be seen during a wiretap and will eventually compromise someone's identity. Hence, this type of communication should be used in lower-level channels, for instance in the channels used to educate trainees who are not yet employed in active campaigns.

Levels of trust

As mentioned previously in this chapter, a growing hacker group can consist of multiple layers of leadership and members. Within these layers different levels of trust and security apply (Fig. 2.1). Members that are new to the hacker group always enter through the level of lowest trust. It is up to



■ **FIGURE 2.1 Example of a communication scheme with different means and methods for communicating.**

the hacker group itself to decide upon the number of layers and criteria for moving between higher and lower layers. When considering criteria for moving up and down in the organization, the hacker group should keep in mind the purpose of the layered structure, namely, the ability to scale and more importantly slow down and mitigate the effects of infiltration attempts. Rising to the highest levels of the hacker group (the core at the top of the pyramid) should take long, as this is the highest level of trust. The member should been an active member; he should have been engaged in operations frequently and proven to be a trustworthy member.

Although it is of utmost importance to prevent covert agents from entering the core group, fear of such situations should never be leading when conducting operations. Fear will only cause panic and false accusations, ruining the morale within the group and generally reducing the effectiveness of the group since it is fighting itself instead of the opponent. The threat

of infiltration is always present; taking basic safeguards, such as levels of trust and security, should dissuade most infiltrators or mitigate the impact of these individuals on the group.

Forums

Apart from IRC channels, the hacker group can decide on using forums as their primary communication channel. Most of the aspects discussed at IRC will also apply to forums; this section will highlight some additional points of interest. Should the hacker group decide to use a forum as its primary communication channel, once again infrastructure of the highest reliability grade should be chosen (see the section on infrastructure). The downside of using forums is that all messages are stored on a server and encryption is less useful. It is very easy to create very specific rules and regulations on a forum; this way trainees and recruits can be guided and protected closely. Forums can be very useful for spreading knowledge among members, trainees, and recruits, for instance, by posting instruction guides, how to's, instructional videos, and other useful informative posts.

Access to the forum should always be regulated. The forum should be structured to distinguish core members and new (potential) recruits that have restricted access to the forum. The parts recruits have access to should be those parts where they are able to showcase their skills and show their eligibility for the hacker group. Core members tasked with recruiting (see the section on recruiting) should keep a close watch on this channel. By looking at the conversations they can easily spot and differentiate between fraudsters and new promising members. As mentioned at IRC, compromising details (eg, information on operations, personally identifiable information, etc.) should never be posted on the forums.

Mobile phone messengers

The Snowden revelations regarding mass surveillance sparked a lively secure messaging ecosystem on mobile platforms. These so-called "secure messengers" on mobile phone platforms can be used to exchange information in a hacker group. There are, however, several things to be kept in mind. Mobile phones, especially smartphones, collect and transmit tremendous amounts of metadata. Using metadata, it is quite easy to forensically determine communication has taken place. Apart from that, it is also rather easy to generate insight about who was communicated, at what location, and how much data have been sent. These secure messengers may protect from mass surveillance; they do not, however, protect members against targeted surveillance. As such, a hacker group member should always be aware of the information communicated by using the mobile platform.

VPNs and CloudFlare

An increasing amount of people hide their online identity and location through virtual private networks (VPN). Services such as CloudFlare provide an extra layer of security. However, it is paramount to realize that using a VPN is not a silver bullet—hacker group members can still be profiled when using a VPN. As such, it is unwise to trust a VPN wholly for providing anonymity, secrecy, and security. Hacker group members should be aware that almost all VPN providers cooperate with law enforcement and other investigatory agencies. Most VPN providers keep logs of their users' activity. These logs provide law enforcement with extremely valuable information; these logs can potentially compromise hacker group members, supporters, and operations. Therefore, the hacker group should avoid using commercial VPN providers, even those that say they delete logs or do not keep logs.

Another widely used platform is CloudFlare. Although it might be beneficial to some users, the hacker group should avoid CloudFlare at all times. There are strong indications that all information being transferred over the CloudFlare network is intercepted and decrypted by investigatory agencies. As such, the hacker group should avoid using this popular service.

Unconventional means and methods

Besides the conventional tools such as TOR, IRC, forums, and websites there are many unconventional means for communicating. These are the types of means not specifically intended for communication but which can be used to send a message. One example is the use of tags (graffiti) in online multiplayer gaming to exchange information. Games such as Counterstrike enable users to create custom tags. Entering the same multiplayer session enables two persons to exchange information. Apart from that there are many other unconventional ways of communicating, for instance using steganography on images and sharing these on inconspicuous-looking online channels (eg, Instagram). Or using the comment boxes on popular websites for sharing information (eg, YouTube comment boxes). The number of potential channels is only limited by hacker group members' ingenuity and creativity.

Recruiting

The hacker group derives its strength from its members; as such, it should always be on the lookout to recruit new members. A member of the hacker group should be assigned specifically for this recruiting task. This recruiter is responsible for recruiting, selecting, and approving new members. The hacker group should put in place a very secure process for recruiting, assessing, training, and educating new recruits.

To someone who knows what to look for, it is easy to spot talented and promising recruits. One can never become a good hacker if experimenting with technology is not in their veins; apart from ideological and intellectual capacity this is one of the core characteristics defining a hacker. Note that hackers who destroy computers, extort, or steal property are not potentially interesting to the hacker group. These individuals have a financial motive and are not interesting for the hacker group that is trying to recruit dedicated and correctly motivated hackers.

Upcoming young hackers often hack a lot of machines, usually without getting caught; there are hardly any thorough investigations into computer hacking cases when there was no big theft. Recruiters should work closely with members responsible for infrastructure to find these types of intrusions on hacked infrastructure. The members in the hacker group tasked with acquiring new infrastructure can perform these types of forensic tasks on systems to spot previous intruders on the system.

Once the hacker group identifies a system that has already been comromised it is useless for further use but the system can be extremly valuable for recruiting purposes. Compromised computer systems should be passed on to group members skilled in computer forensics. This group should investigate the system and collect all possible information on the system. The group should report their findings back to the hacker group. Important aspects are the modus operandi of the compromise, tools used, and possibility to trace the individual.

If the hacker group finds an individual eligible for recruitment, his contact details should be gathered. Finding his contact details will not pose any problems as for the hacker group—it is second nature to track individuals on the Internet. The hacker group can then establish contact, which should be done carefully. No compromising details about the hacker group should be revealed on first contact. Contact should be established and expanded very carefully; the steps of becoming a trusted member should take place gradually. The recruit can be tempted to join and rewarded by the hacker group by giving infrastructure, since true prospects of the hacker group are more satisfied with CPU processing power than with cash.

Once infrastructure access is given to a hacker group prospect, the new recruit's skill can be evaluated by tracking his movements on the infrastructure. Attention should especially be paid to very young individuals, as they tend to be ignorant. Young individuals should preferably not take part in active operations. The newly recruited youngsters should be adopted by the hacker group but only be put into action at a later moment, preferably years after recruitment. The fresh recruit often turns out to possess a number of entry points into systems that can be used for an operation. The recruit's

entry points can be transferred to the hacker group and the hacker group can than appoint the right person to perform lateral movement (which will be discussed in Chapter 3). If an entry point of a fresh recruit is used, this recruit should completely transfer his entry point to the hacker group.

No backdoor should be allowed on the entry point provided by the recruit. The more senior hacker group members should carefully check for the existence of backdoors. If a backdoor is found, the loyalty of the fresh recruit can be put into discussion and his position should be reevaluated. If the recruit did transfer his compromise without a backdoor being persistent the recruit should be awarded. The award could for instance comprise technical knowledge (eg, regarding malware or other software) or processing power (eg, on servers).

Once the hacker group has performed the lateral movements starting from the entry point, the hacker who performed these tasks should have a conversation with the recruit. The more senior hacker group member should explain what he did and what the catch turned out to be. All of the movements done by the hacker should be explained in full detail, with full care, and no knowledge should be withheld. This way the recruit receives valuable information for his own good and trust is being established between him and the hacker group. The recruit will feel acknowledged, his entry points are appreciated, and he receives valuable knowledge for his efforts.

Engineering

Apart from the supporting tasks such as infrastructure, recruiting, and communication, the hacker group logically also comprises hackers/engineers. These are the ones dedicated to conducting the actual operations and are highly proficient in their specific fields. There are particular types of hackers/engineers sought after by the hacker group; we will now describe these types and the different disciplines.

The producer

The producer is a very proficient engineer with his own toolset. This type of hacker is required to create entry points and maintain persistence in targeted objects. He is characterized as having a lot of patience and always being eager to work. For this person programming is a lifestyle, hobby, and often professional occupation. This person is extremely skilled in programming, usually in one specific language. Multiple languages can be an added benefit but are absolutely not necessary for eligibility to join the hacker group.

Of particular interest are persons familiar with reverse engineering or programming add-ons for the Windows operating system. Having thorough understanding of the most-used operating system is a skill that often turns out

extremely useful once the hacker group gets stuck at a specifically targeted system. The hacker group can then discuss the problem with the producer and often it will turn out this engineer has the solution to the problem, either in his own toolset or in his extensive knowledge of the operating system.

The viral growth engineer

The viral growth hacker/engineer is characterized as being capable of generating an extremely high volume of compromises. Where many familiar with computers can hack a machine with known exploits, this type of hacker/engineer is talented in a very specific way—he can achieve viral growth. Creating this type of growth requires a skilled and dedicated person. As many now how to create viral growth in theory, many feel that this is an easy task. Bringing this theory into practice, however, is completely different from theorizing about it. It takes a very specific talent to be able to create viral growth in practice.

The viral growth engineer/hacker is capable of achieving viral growth and has proven their ability of doing so. This person does not necessarily have to be as skilled as the producer, as long as he is able to achieve exponential growth. Most often this requires a mixed skill-set comprising social (engineering) and programming skills. Of particular interest are those engineers/hackers that have created viral growth with very common tools (eg, remote administration toolkits).

The creative hacker/engineer

The creative hacker/engineer is a very specific individual as well. He is highly interested in hacking and vulnerabilities; the only difference is that this person knows how to bundle and exploit vulnerabilities in such a way that it improves the effectiveness of known vulnerabilities. For instance, this person can turn a cross-site scripting vulnerability into remote code execution, and this person can bundle unchecked uploads in combination with remote file inclusion into a remote code execution. This is the engineer to which a hacker group should resort to find out-of-the-box solutions for targeting a system. While not being the quickest or most proficient programmer, using sheer creativity this type of hacker/engineer will find the solution to the problem. This hacker/engineer is not known by his awesome programming skills, but by his ad hoc scripts, which have a tendency to always work. Once a goal (target) is set, this is the person who achieves the goal one way or the other.

Forensics

Although forensics might not sound like a particularly relevant discipline to a hacker group, it can be very helpful for a variety of purposes, for instance

recruiting, obfuscation, and intelligence. As such, having a member proficient in digital forensics is essential. As he is proficient in forensics, this hacker group member can provide the hacker group with feedback on using particular code or software. He can easily pinpoint mistakes often made while coding, using malware and advice on minimizing forensic traces. He also knows the modus operandi of forensic researchers and thus knows how to thwart investigations.

Although in the ideal world malware would not leave a single trace, we live in a far from ideal world in which malware always leaves traces. As such, the hacker group should prioritize suggested improvements to reduce the forensic imprint—knowing that investing too much time in trying to reduce the forensic footprint would be infeasible and ineffective. An exception to this practice is leaving easter eggs, ludic clues as to the (fake) identity of the perpetrator, to demoralize or mislead the opposing actor and to prove that the system has been compromised. Besides consulting the forensics member beforehand, this member should also be one of the first to take a look at a hacked target system after initial compromise. He can easily spot mistakes the initial hacker has made and can try or advise on taking precautionary measures or to wipe any residual traces leading to the hacker group.

Besides using the forensics discipline to improve the hacker group's operations, forensics can also gain valuable information from compromised systems. Forensics can, for instance, spot the presence of any other hackers on the system. As mentioned before, spotting another hacker on a target system can be one of the prime resources for new recruits. Although it may sound farfetched, in practice this happens quite often. Should the hacker group find another, nonmember hacker on the system, they should first try to establish why the hacker is on the system and how he has entered. Once the available information is analyzed, the hacker group should decide on establishing contact with the hacker or not. If the hacker proves not eligible for recruitment, the hacker group should still decide on what to do with him as he might compromise the goal of the operation.

One option would be to leave the hacker in the zone he is in; this should only be done if the hacker group has no time or other circumstances do not permit the second option: removing the unknown hacker from the target system. The best course of action upon finding a nonrecruitable hacker is removing him from the network and moving on. This does not mean that the unknown hacker cannot be contacted at a later moment, for instance when the hacker group hits a dead end and requires the hacker's knowledge (and entry points). The hacker group should never disclose the operation to the unknown, noneligible hacker as it might compromise the ongoing operation.

The unknown individual could become selfish and claim the compromise for himself, prove to be an informant or hunting team, or otherwise be detrimental to the operational success of the hacker group.

Should the hacker group feel that the hacker found on a system could be eligible for recruitment, contact should be established in a careful manner. First contact should always be careful; a simple "hello, we are …, who are you?" can be enough to break the ice. Once the hacker group has established that the hacker is not a threat to the hacker group or the operations, it is best to disclose general details on the operation to gain trust. Establishing contact with hackers already present in systems can be of crucial importance to achieve operational success. Since like-minded individuals with knowledge of target systems are rare, the hacker group should carefully consider turning down such an asset; in most cases it is a quick way of recruiting knowledgeable like-minded hackers.

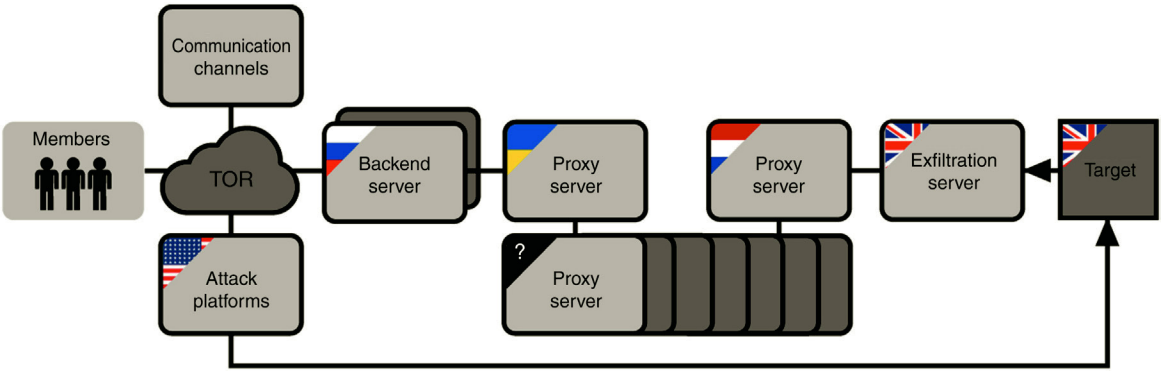
Command and control

Command and control infrastructure should be put in place to exchange or exfiltrate information, manage (attack) infrastructure, and other issues requiring synchronization. Choosing the right command and control infrastructure for an operation can contribute greatly to operational success. Not thinking thoroughly about the command and control infrastructure or misconfigure the infrastructure can compromise the operation and the hacker group.

Data exfiltration

Ideally the command and control infrastructure uses TOR to hide its true physical location. However, the downside of TOR is that the connection often is unreliable and slow. Exchanging merely 1 GB of data can prove to be an excruciatingly slow process; due to connection timeouts and other interruptions one might end up transferring 8 GB just to exfiltrate 1 GB of data. Failing connections increase bandwidth usage and therefore increase detection possibility due to anomalies in network usage. To decrease the fail rate and increase the extraction speed, the ideal setup for command and control infrastructure is setting up as close to the target as possible (Fig. 2.2). The latency between the command and control server should be as low as possible and the Internet connection of the target should be carefully tested to determine the maximum exfiltration speed possible.

If the hacker group is aware of network monitoring tools being present in the network, they should carefully consider the extraction speed and rate. Preferably they should limit (or "cap") the speed to prevent network anomalies from taking place—both volume spikes and dips. The spikes may stand



■ **FIGURE 2.2 Example of an infrastructure configuration required for operations.**

out against normal network traffic, raising suspicion within network administrators. The dips may be noticed by legitimate users as exfiltrating at maximum speed may slow down the network speed for other traffic. The hacker group should carefully determine how to best prevent both spikes and dips while at the same time exfiltrating information as fast as possible.

Call backs

There are many types of malware that need to call back to the hacker group's command and control infrastructure, for instance to exchange data, receive updates, obtain instructions, or any other type of communication. The malware left on the systems should connect to an address that can be resolved via the DNS. Peer-to-peer could be considered, but it should be kept in mind that peer-to-peer traffic can be easily spotted on a network.

Malware planted on systems could contain domain names and backup domain names. If backup domains are used it is recommended to use different registrars in different jurisdictions to prevent effective coordinated takedowns. Another approach is to continuously download new backup domain lists. The new gTLDs are an outcome as well; the organizations operating these new TLDs are often new to the business and therefore lack connections and abuse departments. This is ideal to keep your domain online as long as possible.

Another way of keeping command and control infrastructure or systems running longer is using fast flux domains. The hacker group should, however, keep in mind that when transferring large amounts of data this does not provide an extra layer of security—the endpoint will be easily detected.

Domains should always be registered anonymously; some TLDs require business licenses or identification. It is very easy for the hacker group to obtain business licenses or fake identification papers that could be used to purchase these domain names. Once a domain name or server is purchased, the hacker group should be aware that the registrar shares all information with third parties. From the moment you register, Google's and other search engine's crawlers will start to index the domain. Therefore, the domain should be the last thing to be registered; first the other infrastructure should be put in place and appropriate security measures taken.

A mistake that is often made is attaching static infrastructure to the domain name to check if everything functions before conducting an operation. The hacker group should be aware that all IP addresses connecting to the domain are logged and available for later requests. All IP addresses ever attached to a domain end up in databases that are accessible for forensic researchers. These databases often provide extremely valuable information regarding the identification of hackers.

Proxies

The hacker group should always use a layered proxy setup (Fig. 2.2). The first proxy server should be the server closest to the target. This server basically serves as a relay server. Once data gets onto this server they are (ideally) forwarded to multiple locations. The benefit of this server is that there is no need for a speed limitation and therefore a server should be chosen with maximum bandwidth capacity. This relay server is the first server to be taken down if the operation gets discovered; hence the hacker group should aim to reduce the amount of data stored on this server. This can be achieved by forwarding exfiltrated data as quickly as possible to another proxy server or a backend server.

It is best for the hacker group to use disposable infrastructure. Ideally infrastructure should not be reused; after an operation the hacker group should dispose the used infrastructure. Members tasked with forensics should make sure the infrastructure is forensically wiped or at least aim to reduce traces. When considering the location of infrastructure, including proxy servers, the hacker group should try making investigation as hard as possible. One of the most effective things to frustrate investigations is using infrastructure from different legislation. To maximize the effort needed to investigate, the hacker group should preferably select Countries with completely incompatible legal systems or Countries that do not get along well. One can imagine, for instance, that a request for assistance from the United States of America to Russia takes longer to satisfy than

one from the United States to the United Kingdom. The longer this timeframe can be stretched, the better for the hacker group.

Backend server

The backend server is the most important server during the whole operation (Fig. 2.2). This server can be one or more servers, depending on the operation. This server is used by the hacker group for collecting, curating, and analyzing retrieved data. To do this as fast as possible, backend servers should ideally have enough memory and especially disk space. To prevent data loss, the hacker group can consider creating a backup of the backend server, possibly offline.

Developers

Developers play a crucial role within the hacker group. The difference between a hacker and a developer is that the hacker creates "quick and dirty" tools while the developer takes more time to create a near-perfect tool which may be reused. It takes a lot of time, however, to develop effective tools that can be used by the group's hackers or engineers. In some cases, when operational circumstances permit more preparation time, the hacker group can task developers with building tools. Ideally the hackers instruct the developers and specify their requirements; the developer should then translate these needs into efficient tools.

External communication

Members tasked with external communication are the ones responsible for creating content for the various external communication channels maintained by the hacker group. As there are many possible channels using different media, this discipline will most likely be fulfilled by multiple members with a specific skill or one very skilled creative designer (eg, video editing, web design, illustration skills, etc.). Most essential for the hacker group is to have a skilled web designer capable of creating visually and technologically sound websites. This member masters languages like PHP, ASP, Ruby on Rails, CSS, Java, and most importantly HTML. The web designer is of utmost importance to a hacker group for creating and maintaining appealing communication channels—for instance websites. Besides building a website this member can be used to design other content for social media and forums. He can also be used to create phishing mails and websites or other content needing to be visually tailored to a specific target.

Press relations

The press relations (PR) subdiscipline of external communications is aimed at furthering the hacker group's goal by mobilizing support for the hacker

group and denying support to opposing actors. The member(s) tasked with PR should maintain contacts with conventional press and maintain a firm foothold on social media. Of course, it depends on the context whether it is viable to use social media, conventional media, or both. The use of media will be exemplified further in Chapter 3 (media strategy). This section will, however, emphasize an essential activity for PR discipline: maintain contacts with reporters.

Reporters should be picked with utmost care since they can make or break an operation. The hacker group should carefully select a trusted base of reporters and establish a relation with them. These reporters can be selected on basis of their mind-set and audience, for instance activist journalists or neutral journalists with a large audience. Once there is a level of trust between a reporter and the hacker group, the relation can be enhanced by awarding the reporter with scoops and insider information. By doing so, a trust relation and mutual dependence will be established, which can be very extremely valuable to the hacker group. The value and impact of these types of cooperation become apparent when considering the mutually reinforcing relation between Edward Snowden and Glenn Greenwald.

The hacker group should aim to keep the trusted reporter base up to date regarding their operations, of course, only when exposure is beneficial to the hacker group. To keep them updated, they can be invited into communication channels (eg, IRC) or send an information package regarding a successful operation. By giving the reporter access to information, he will evaluate the newsworthiness of the content and could probably assist in creating a "product" that is more newsworthy.

CONCLUSIONS

This chapter has discussed the type of individual and mind-set required to conduct cyber guerilla. It has discussed the intellectual and ideological capacities a cyber guerilla should possess, best characterized as the hacker as social reformer and combatant. After that it has focused on the organizational aspects of the hacker group and distinguished various disciplines for conducting operations. Skillful and motivated group members and efficient organization enable the hacker group to conduct operations. The following chapter will offer the hacker group concrete footholds for conducting operations.