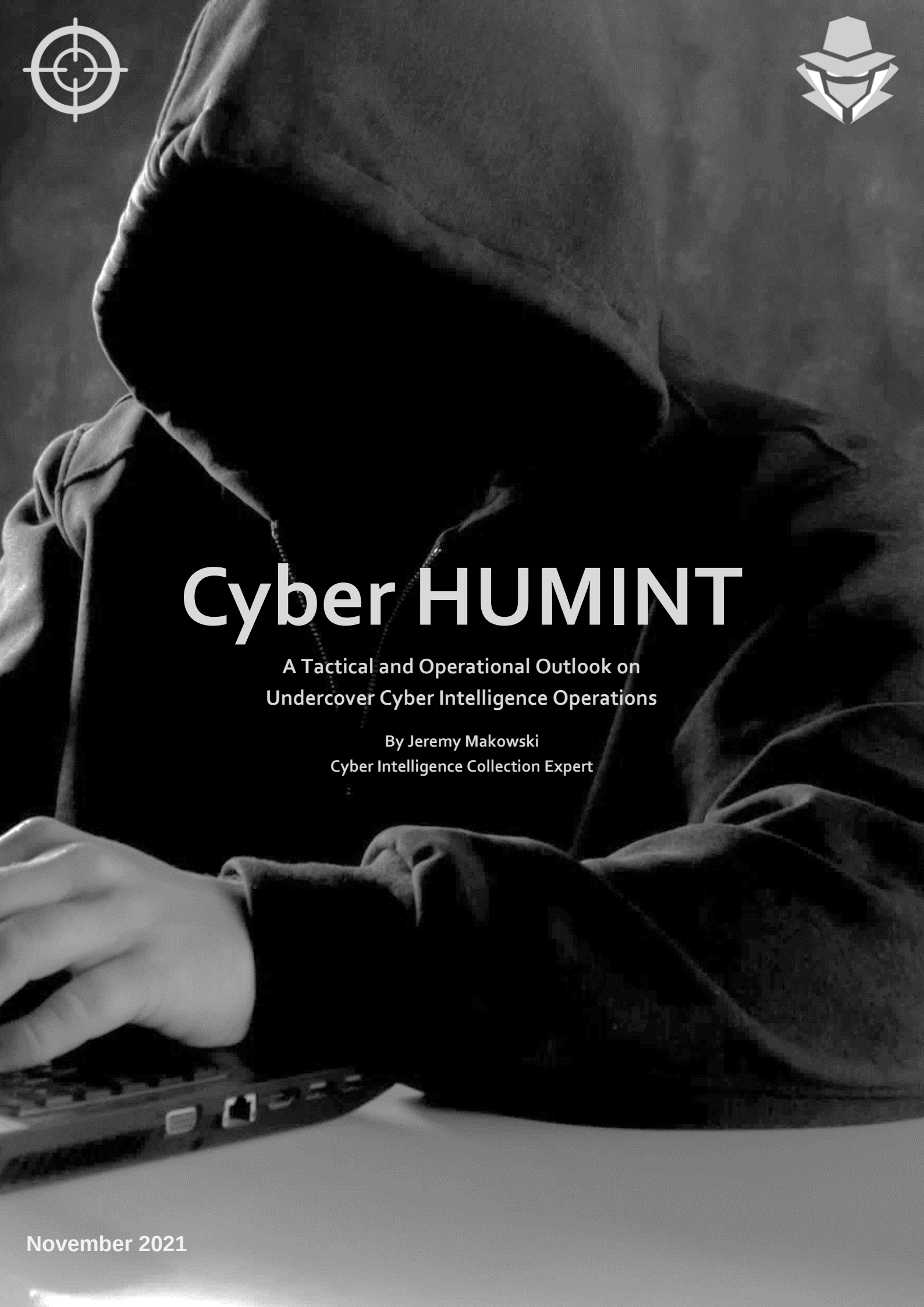


Cyber HUMINT

A Tactical and Operational Outlook on Undercover Cyber Intelligence Operations

By Jeremy Makowski
Cyber Intelligence Collection Expert

November 2021

Table of Contents

1. Introduction

With the emergence and development of social networks, forums, boards and encrypted messaging applications, cyberspace became a vaste battlefield made up of different types of threat actors. On a daily base, they use it to disturb, compromise or destroy national critical infrastructures, private companies as well as financial institutions . While most of governments and private companies have understood the challenges of cybersecurity and adopted its culture, the use of cyber intelligence and more particularly Cyber HUMINT remains insufficiently used, despite the emergence on the market of several companies offering cyber intelligence collection's systems and services.

It is important to distinguish between the different aspects of cyber threat intelligence and their added values. Cyber threat intelligence is a discipline that brings together several areas including: network and threat intelligence (packet analysis and reverse engineering), OSINT (surface web and open source collection) and Cyber HUMINT (deep sources collection with human interaction) . All of these areas each have their own advantages and specificities. However it is important to notice that Cyber HUMINT is the only area considered as active because it requires a virtual human interaction which makes it so special.

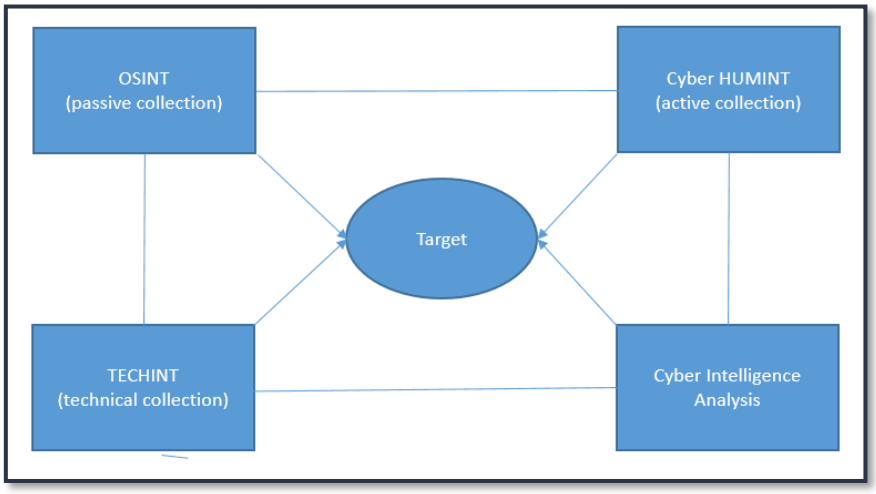


Figure 1: connection between the target and the different intelligence steps

2. What is Cyber HUMINT ?

Cyber HUMINT is the use of traditional HUMINT techniques and methodologies coupled with the use of computer tools and skills to identify, recruit, manipulate and gather information on sources or targets operating online. Cyber HUMINT takes advantage of the human factor, using different techniques such as:

- Social Engineering.
- Natural Language Processing.
- Psychology.
- Negotiation Techniques.

Cyber HUMINT requires a deep understanding of the intelligence world as well as the cyberspace and its different threat actors. For military or law enforcement intelligence specialists, Cyber HUMINT is a great methods to identify and collect information on the activities and modus operandi used by cybercriminals and terrorists targeting critical infrastructures and national institutions. On the commercial side, civilian intelligence analysts mainly use Cyber HUMINT to actively collect information on threat actors seeking to target private companies and financial institutions. The fundamental difference in the use of Cyber HUMINT between governments and private companies reside in the fact that governments are usually more interested in identifying threat actors to sue or target them back, while private companies are more interested in gathering intelligence on threats and vulnerabilities to help their clients to protect their business, IT infrastructures and improve their cyber security policy.

3. HUMINT vs Cyber HUMINT

Traditional HUMINT uses a set of skills and methods which are applicable in the physical world such as behavioral analysis or body language. These techniques and methods allow HUMINT professionals to identify and draw up the profile of their interlocutor. Indeed, when a HUMINT specialist meets a source, in a few hours they can realize the type of person he has in front of him and thus activate levers that will allow him to bring his interlocutor to give him the information he needs. Unlike traditional HUMINT, Cyber HUMINT has a different approach due to its environment. If during a tradditional HUMINT operation an intelligence officer can physically analyse the behaviour of its source/target by using techniques such as body language or behaviour analysis, it does not work when it comes to Cyber HUMINT operation. A non-physical contact allows a much smaller field of possibilities. However, it is possible to try to identify the origin of a threat actor by paying attention and analyzing certain details such as the language used by the threat actor as well as its syntax. If Cyber HUMINT and HUMINT have differences, these two disciplines are also very complementary. When a HUMINT specialist operates on the field he may collect from a source useful information such as email addresses or nicknames that may be useful for a cyber HUMINT specialist.

HUMINT	Cyber HUMINT
Physical Space	Cyber Space
Nickname	Avatar/Moniker
Physical human contact	Virtual human contact
Body language and physical behaviour analysis	Natural Language Processing and online behaviour analysis

4. Cyber HUMINT and OSINT

OSINT is the process of passive data collection on threat actors and their activities from various sources (mostly digital). Today unlike Cyber HUMINT OSINT is mainly carried out automatically. Many global cyber security companies offer automatic intelligence collection systems which collect data from the surface web to the darknet. These systems are usually using artificial intelligence as well as link analysis and specific patterns in order to collect different types of data (e.g. name, nickname, address, phone number, IP, email, crypto currency addresses, IOC…). Usually a cyber intelligence gathering process begins with the collection of data by using an automatic intelligence collection system in order to have a first view of the exposed assets and threat actors targets.

This step can possibly be followed by a Cyber HUMINT operation if the information collected by the OSINT automatic system is sufficiently relevant and consistent. Cyber HUMINT is an intelligence discipline that has proven itself and continues to contribute to the fight against different types of crime and terrorism activities in all its forms (traditional and digital). It helps to identify threat actor, their modus operandi and can be effective in the prediction of potential future cyber attacks.

5. Cyber HUMINT: Understanding the Cyberspace and its different aspects

5.1 Networks and Infrastructures

Before being engaged in a Cyber HUMINT operation, a deep and good understanding of the cyberspace is required. It is therefore important to know about the environment in which we are going to operate in order to become familiar with the infrastructures and the sources which defines it. Cyberspace is divided into three different subspaces the Surface Web, the DeepWeb and the Darknet.

The Surface Web refers to the internet and is accessible to the general public with a simple web browser and a classic search engine such as Google Chrome, Internet Explorer or Firefox. The surface web gives access to all general and widely open sources such as Facebook, Youtube, Instagram, Gmail…The surface web is exploited and used by different threat actors with different aims.

The Deep Web refers to the largest part of the internet which is not indexed by regular search engines such as Google Chrome. Around 90% of the sources on the internet are not indexed by Google. Indeed many web pages are considered to belong to the Deep Web as they do not use common top-level domains (TLDs), like .com, .co, .org, and are not indexed by regular search engines. The sources on the deep web are

usually services that require a restricted access such as, online banking, mail servers or social media private pages. From the infrastructure perpective, deep web websites are reachable by regular URL or IP address, however they can require to go through a secure access (user/password) in order to reach public-website pages.

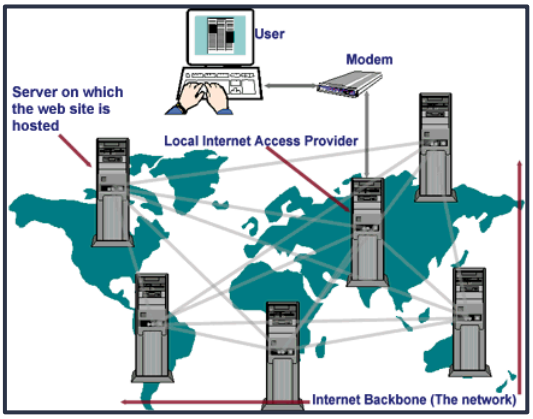


Figure 2: Internet network architecture (open source)

The Darknet refers to underground networks which are overlayed to the internet. The darknet is reachable with the help of a specific browser or software. The most popular networks of the Darknet are The Onion Router (Tor) and The Invisible Internet Project (I2P). These two browsers allow to access underground websites which are usually indexed by repositories and search engines. The main goal of these networks is to remain anonymous and keep privacy with the help of advanced encryption systems. However most of the darknet sources (forums, markets, boards, automatic shops, paste sites…) involve cyber criminal and terrorist activities. In terms of cyber criminal activities, the darknet is more often the playground of gun and drug dealers as well as pedophiles rather than advanced hackers. Indeed forums and markets offering hacking services, vulnerabilities or malware are of low level and cannot be compared to hacking forums of the deep or surface web. Additionally the stability of the darknet is relatively weak. Many of the forums and markets do not last more than one or two years for multiple reasons (takedown by law enforcement, multiple DDoS attacks, or lack of users and activities).

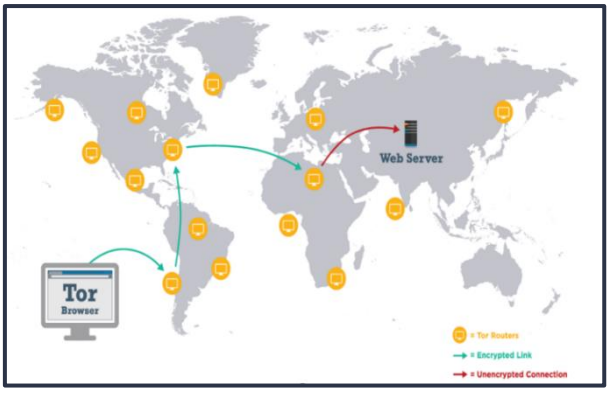


Figure 3: The TOR network infrastructure (open source)

5.2 Sources and Data

Sources are one of the key points to a successful Cyber HUMINT operation. They are the place to be in order to identify relevant threat actors and threats. They are varied and can take several forms such as: social networks, paste sites, forums, boards, markets, encrypted messaging applications…

Figure 4: Some Web, Deepweb and Darknet sources (open source)

- **Social Networks**

Social networks are the sources with the largest number of active users in the world since they have several billion. They are hosted and operates within the surface web and have widely multiplied in recent years. Today beyond Facebook and Twitter, there are multiple social networks specific to particular domains or languages. To conduct an effective Cyber HUMINT operation, it is important to understand that social networks have their own rules and work methods. Some of them would require to have a well structured and active profile to avoid looking suspicious and getting blocked. To maintain a good profile on social networks, it is important to be active and consistent in your behavior and online activities. The information on social networks can be divided into two categories public and private. Public contents are accessible to everyone while private contents have undergo privacy policy and cannot be accessed without the approval of its writter. In order to gather intelligence from restricted profiles or groups, Cyber HUMINT is probably the best way. With a well structured real fake profile it is possible to approach and be connected to a threat actor in order to access his private information and published content.

.

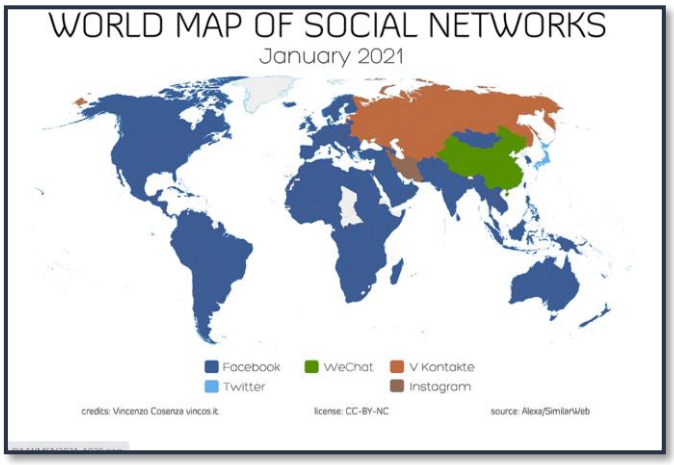


Figure 5: World map of social network 2021 (source: VINCOS)

- **Forums**

Forums are certainly the most interesting sources when it comes to hacking and cyber crime. While social networks are the battlefield of hacktivists, forums are clearly the land of cyber criminals. There are hundreds of forums and they are all different depending on their sizes (e.g. number of posts, number of users) speciality (e.g. hacking, financial fraud, data leak...) as well as languages (e.g. French, Spanish, English, Arabic, Russian, Chinese, Persian ...). Moreover some forums are more exclusive and private than others as they require entrance fees or knowing a forum member who can vouch for you to become a new member.

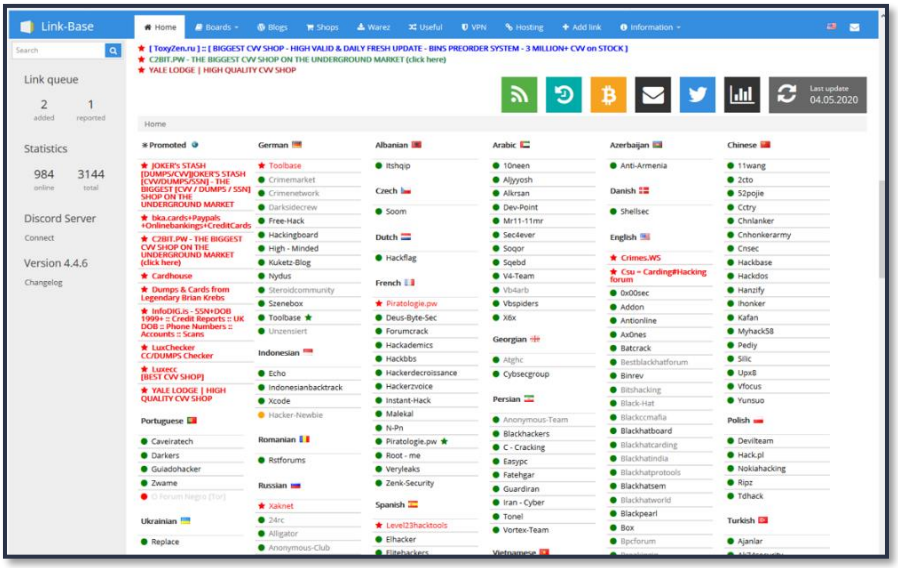
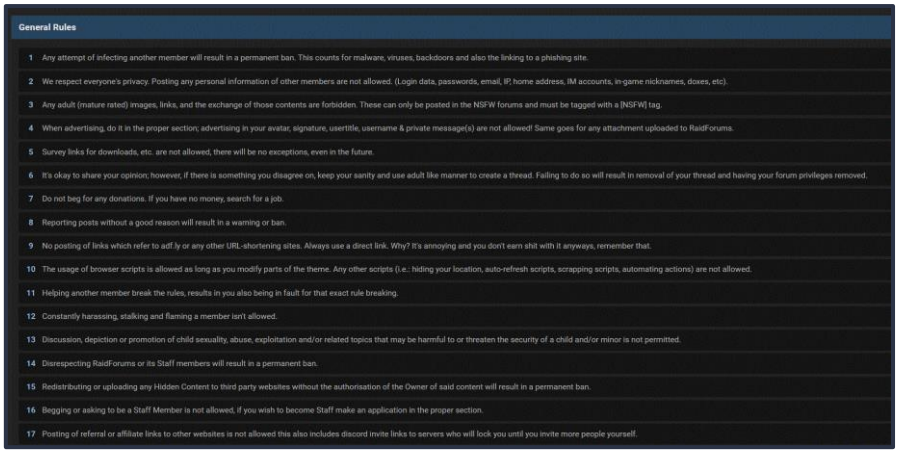


Figure 6: : A list of hacking / cybercrime forums from all over the world (source link-base)

Each forum has its own rules and internal policies that help understand how to behave towards users and administrators. To conduct an effective Cyber HUMINT operation on a forum, it is important or even essential to know these rules and to understand what is possible or not.



General Rules

1. Any attempt of infecting another member will result in a permanent ban. This counts for malware, viruses, backdoors and also the linking to a phishing site.
2. We respect everyone's privacy. Posting any personal information of other members are not allowed. (Login data, passwords, email, IP, home address, IM accounts, in-game nicknames, doxes, etc).
3. Any adult (mature rated) images, links, and the exchange of those contents are forbidden. These can only be posted in the NSFW forums and must be tagged with a [NSFW] tag.
4. When advertising, do it in the proper section; advertising in your avatar, signature, usertitle, username & private message(s) are not allowed! Same goes for any attachment uploaded to RaidForums.
5. Survey links for downloads, etc. are not allowed, there will be no exceptions, even in the future.
6. It's okay to share your opinion; however, if there is something you disagree on, keep your sanity and use adult like manner to create a thread. Failing to do so will result in removal of your thread and having your forum privileges removed.
7. Do not beg for any donations. If you have no money, search for a job.
8. Reporting posts without a good reason will result in a warning or ban.
9. No posting of links which refer to adf.ly or any other URL-shortening sites. Always use a direct link. Why? It's annoying and you don't earn shit with it anyways, remember that.
10. The usage of browser scripts is allowed as long as you modify parts of the theme. Any other scripts (i.e.: hiding your location, auto-refresh scripts, scrapping scripts, automating actions) are not allowed.
11. Helping another member break the rules, results in you also being in fault for that exact rule breaking.
12. Constantly harassing, stalking and flaming a member isn't allowed.
13. Discussion, depiction or promotion of child sexuality, abuse, exploitation and/or related topics that may be harmful to or threaten the security of a child and/or minor is not permitted.
14. Disrespecting RaidForums or its Staff members will result in a permanent ban.
15. Redistributing or uploading any Hidden Content to third party websites without the authorisation of the Owner of said content will result in a permanent ban.
16. Begging or asking to be a Staff Member is not allowed, if you wish to become Staff make an application in the proper section.
17. Posting of referral or affiliate links to other websites is not allowed this also includes discord invite links to servers who will lock you until you invite more people yourself.

Figure 7: A list of internal rules and policy from an En glish speaking hacking forum (source: Raidforums)

- **Markets**

Underground markets give cyber criminals the opportunity to trade in illegal products. Each market allows sellers to have a shop within the market. Sellers typically offer for sale: credit cards, bank logins, exploit kits, malware, personal identity information, drugs, weapons, counterfeit money, and documents. Usually each seller has a profile with the details of the products they sell and most of the time their PGP encryption key so buyers can send them private message and encrypt the marketplace. Additionally, sellers can be rated based on the quality and service they provide. However, it is important to understand that some sellers open multiple accounts and play with their avatars by writing positive reviews to increase their reputation.

Before being engaged in a Cyber HUMINT operation on an underground market, it is important to be aware that there are many scammers. In order to evaluate the risk and the efficiency of the operation, it is preferable to check the reputation of a vendor on forums which deal with underground darknet markets (e.g. The HUB forum). It is also important to know that darknet markets do not have long term stability as they are either suppressed by law enforcement, targeted by DDoS attacks as well as modification of hosting service and onion link.

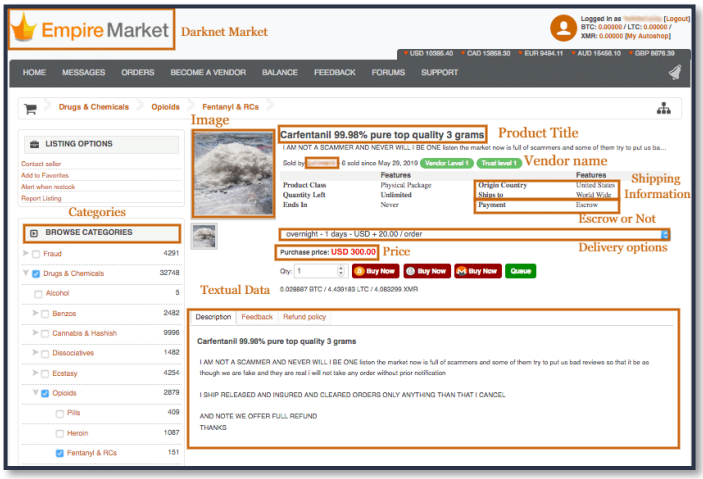


Figure 8: Profile of a vendor on a darknet market (source: empire market)

- **Encrypted Messaging Applications**

With the proliferation of data collection operations led by governments and some private companies, many encrypted messaging applications have emerged. However, if on one hand these applications provide users a secure and private way to communicate they are also a powerful tool for cyber criminals and terrorists..If these applications seems to be a serious issue for law enforcement and intelligence agencies, they are also excellent sources for gathering intelligence on threat actros TTPs. Many of them use these applications to communicate with each other, make deals and recruit people for criminal or terrorist activities. Before being engaged in a Cyber HUMINT operation, it is important to familiarize yourself with these applications, their specifities and components. In addition, a good understanding of the applications used by different communities is also important. For example, some threat actors active in Russian-speaking forums prefer to use a certain type of applications such as Jabber and Telegram, while others prefer ICQ, Discord or Skype.

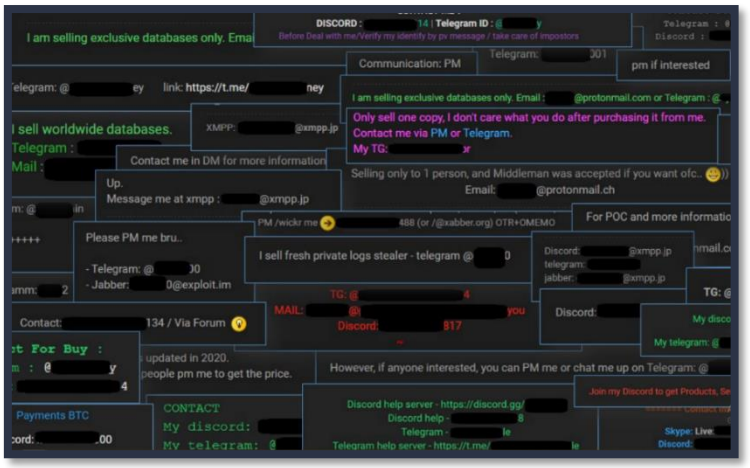


Figure 9: Some contact examples published by Threat Actors on different forums (source: Bank Security Info)

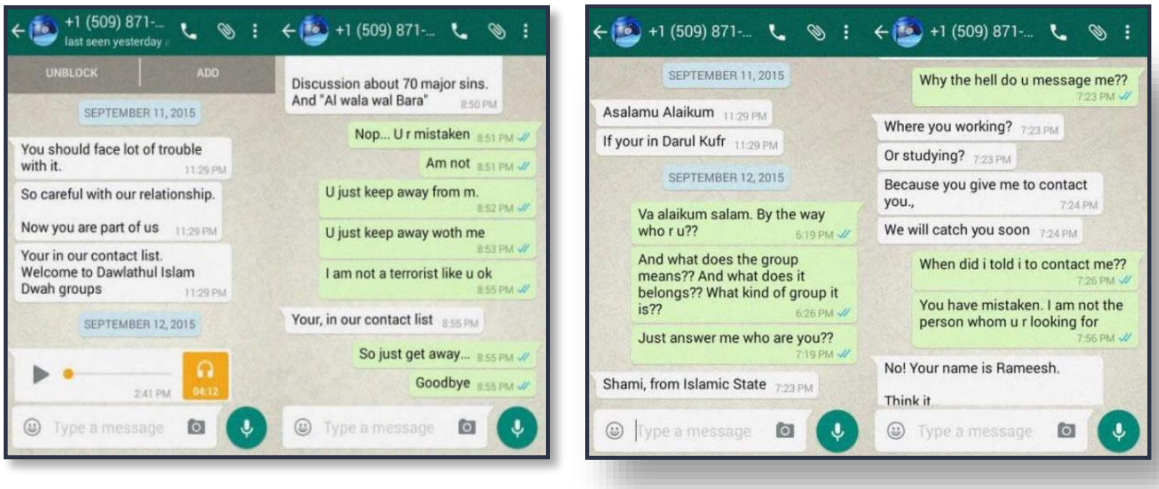


Figure 10: A Whatsapp conversation between a member of the ISIS terrorist group and a potential recruit (source: MIRCHI9)

Currently Telegram is probably one of the the most popular applications used by cybercriminals and terrorists. This application provides an end to end encryption service as well as hiding the phone number used by the application. This application allows certain functions such as secret chat mode which allow to send secure messages with an auto-erase function after a few seconds or minutes. Moreover, telegram allows to create different groups and channels that are used by threat actors as a way of promoting their ilegal items, ideology or recruiting people. If the proliferation of private and public groups on this application can be seen as a problem in terms criminal and terrorism activities, they are also very good sources fto find relevent information on threat actors' activities. Encrypted messaging applications have enabled threat actors to target a wider audience since they are mainly used from smartphones. This mobility has taken precedence over the use of the TOR network which, even with a smartphone version, remains more complex to implement and use, rather than Telegram or other secured messaging applications.

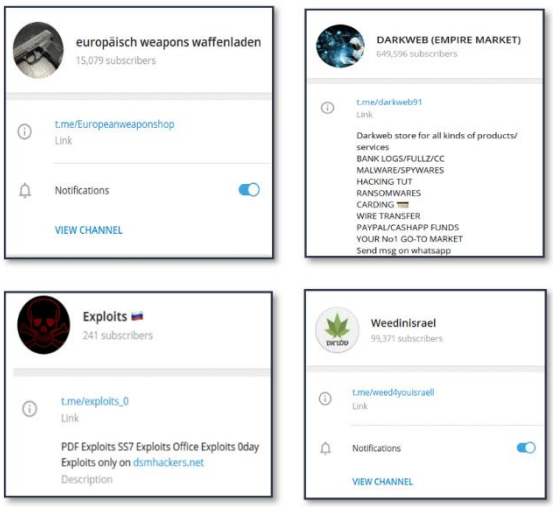


Figure 11: Some exemples of Telegram's groups dealing with weapons, drugs, exploits, malware. (open source telegram)

6. Cyber HUMINT: Understanding the Different Threat Actors' Profiles.

6.1 Cyber Criminal

In recent years, the significant increase in cybercrime activities has led to the development of intelligence collection methodologies on cyber threats. The world of cybercrime is made up of different actors with different activities including: malware developer, botnet operator, hacking infrastructure manager, technical support, bank dropper, carder, money laundering expert as well as people managing cybercrime forums. Each cybercriminal community has its own culture, codes, slang and working methods. A Russian hacker will not have the same behavior as an Arab, Spanish or French hacker.

When talking about the Russian cyber criminal community it is important to note that it refers to Russian-speaking threat actors and not just those from Russia. The Russian language is actively used by many threat actors from FSU countries. Thus among the Russian-speaking hacker community we can find Ukrainian, Belarussian, Moldavian, Latvian or Kazakhstan threat actors. However we will notice differences in language and slang used by these different threat actors. Indeed by speaking with Russian-speaking threat actors, it is possible to identify certain words or expressions used by one population rather than another.

Russian-speaking threat actors generally prefer to deal with people who speak their language. They generally behave in a reserved or cold manner and not let their emotions and details about them show through. Moreover they are good businessman who honor their deal but but do not like to waste their time. Russian hackers operate on several Russian speaking forums where they are mainly focus on malware, vulnerabilities, exploits kit and other technical tools. Usually the most interesting and highly skilled hackers operate on close forums that can be accessed either by entry fees or by connections depending on their policy. While being engaged in a Cyber HUMINT operation in order to gather significant information on Russian speaking threat actors, a high level of technical knowledge as well as good connections are required. It is also strongly preferable to speak Russian to interact with them. It is not impossible to establish a trusted and durable relationship with Russian hackers if you do not speak Russian. However It will probably take more time, resources.

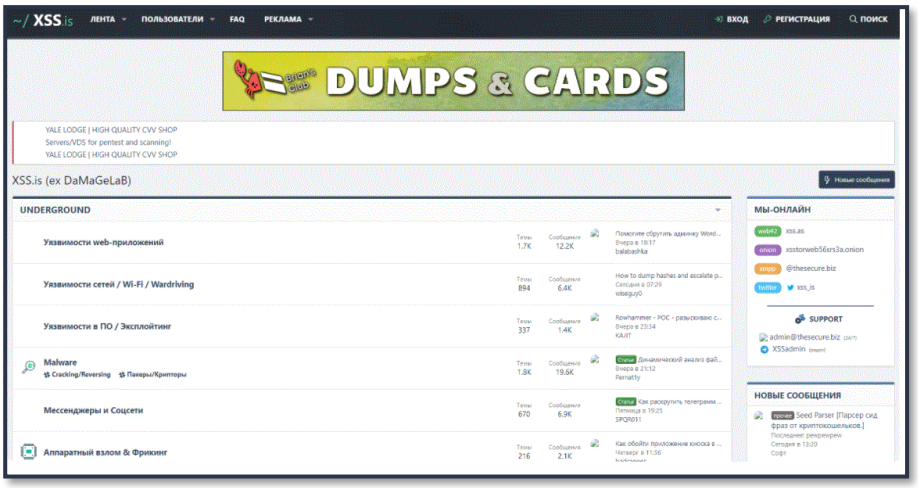


Figure 12: One of the top Russian speaking hacking forum (source: xss hacking forum)

In recent years a large wave of ransomware attacks has been observed. Private companies as well as nation state critical infrastructures from all over the world have been affected by ransomware. Most of the time they have been sent by Russian-or Chinese threat actors. While most governments do not agree with the principle of paying a ransom, during a ransomware attack on a hospital or vital infrastructure, Cyber HUMINT can be considered as an option to try to negotiate the price of the ransom and to collect information on the identity of the threat actor operating the ransomware. In the framework of negotiations with cyber criminals, it is important to underline that people trying to negotiate the price of the ransom should be professionals that know how to negotiate but that also know the cybercrime world. The stress caused by the attack gives cybercriminals a certain psychological edge on their victims who can make mistakes if they decide to negotiate on their own. Indeed in some cases the victims trying to negotiate may say things which can anger the cyber criminals and thus cause an increase in the ransom. When negotiating, certain techniques can be used such as:

- Try to generate empathy from the hacker (especially when the victim is a hospital or a small company without large financial resources).
- Compliment the hacker for his exploits.
- Establish a business relationship (win-win).

Unlike Russian speaking threat actors, those from Arab countries usually have a more flexible behavior. They are generally more open to discussion as they like to show their capabilities. It will generally be easier to discuss and try to extract information from an Arab speaking hacker rather than from a Russian one. On the other hand, Arabic-speaking threat actors can be seen as persons not always trustworthy. Indeed they do not always honor their agreements or promises, meaning that some of them will scam or provide information or services that are not always worth the price they ask for. Their behavior and motivations often reflect a certain mix of genres. Most of the Arabic-speaking forums present a combination of religious and socio-political references as well as technical and hacking aspetcs. Many Arab-speaking threat actors are often either nationalistic or claim their Islamic identity. They generally have no problem having discussions with other non-Arab-speaking threat actors, but it is true that to infiltrate threat actor groups on Arab hacking forums, it is much easier to be Arab-speaking.

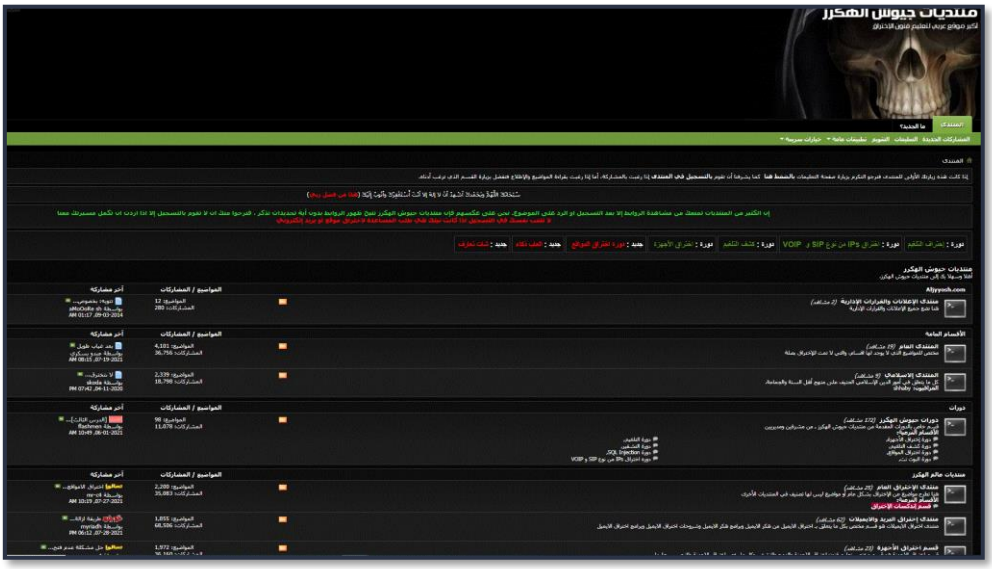


Figure 13: An Arabic speaking hacking forum (source: Aljyyosh hacking forum)

Like Arabic English-speaking threat actors (which generally include european threat actors) are usually open to discussion but have a certain reserve, more or less depending on their nationality and culture. It is also well known that many threat actors from South America, Asia and the Middle East are also active in English hacking forums. Usually, it is easy to recognize those who are non-native English speakers due to the vocabulary and expressions theu use. Some non-native English speakers use online translation of their own language, but this does not necessarily translate well into English.

Figure 14: One of the most famous English sphacking forum (source: hackforums)

The Chinese hacking community is less open than the Russian, Arab or English ones. It is extremely difficult if not impossible to conduct a Cyber HUMINT operation on Chinese threat actors when not being a Chinese speaker. Additionally a deep understandong of the Chinese hacking community environment is required. Indeed they have their own specific ways of communication (QQ, WeChat...) and do not use the popular ones like other communities. Chinese forums generally require members to be active before being able to make some deals. Some state limitation of the content of these forums makes it more difficult to find interesting information than on Russian forums. Moreover unlike on Russian-speaking hacking forums, there are no active English speakers on the Chinese ones.

Figure 15: A Chinese hacking forum (source: Card Fan Chinese forum)

This view on the different comunities is an observation after carrying out multiple Cyber HUMINT operations with threat actors from different countries and cultures. However the personality and character of each threat actor, regardless of his country of origin and his culture has an important part on his behavior.

What are the different steps to perform before being engaged in a deep Cyber HUMINT operation regarding cyber criminal activites?

- Identifying the different forums where the targeted threat actor is active.
- Understanding the threat actor expertise (e.g. hacking, carding, money laundering, weapons, drugs...).
- Be sure to have the right technical, professional knowledge and skills relevent to the operation.
- Preferably speak the language of the threat actor.
- Building a strong cover story as well as a good a profile with some relevant threads and posts that can be found on various cyber criminal forums.
- Make sure to have the right ways of communication depending on what the targeted threat actor uses (Telegram, Signal, Whatsapp, Jabber ...).

In a Cyber HUMINT operation it is sometimes possible to identify things such as the ability and willingness of the threat actor to engage in dialogue. Indeed, if the size of his sentences is short it may reflect a certain reluctance to open up and have a dialogue. On the other hand, if the questions asked to the threat actor are rather short and his answers are longer with some details about his activities and techniques, it shows an openness and a greater willingness for communication. While there is no absolute rule in terms of Cyber HUMINT techniques, it is nevertheless recommended to adapt to your interlocutor. It is often good to go in his direction by adhering to his ideas and/or by complimenting him on his technical and professional skills. This usually greatly increases the chances of obtaining information or contacts which only the threat actor can provide.

6.2 Hacktivist

Hacktivism is a phenomenon which began to be significant in 2003 with the creation of the decentralized movement Anonymous. This term of hacktivism (contraction of activism and hacker) was then "democratized" with the emergence of Facebook in 2006 and other social networks such as twitter, Youtube , Instagram, tiktok and VK. Hacktivists have seen in social networks the opportunity to broadcast their religious, political or social ideological messages by creating cyber attack campaigns and publishing the results of these attacks (website defacement, database leak ...). For hacktivists, social networks are an important way of communication which allow them to reach a large number of people.

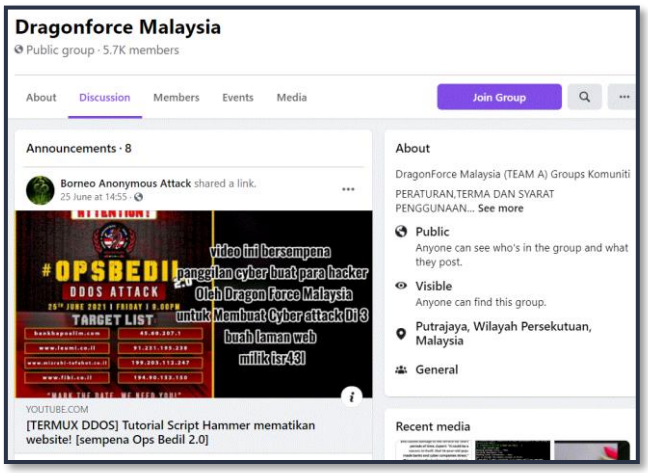


Figure 16: The Facebook page of the hacktivist group Dragonforce (source: Facebook)

Moreover it has given them the opportunity to unify their forces and get more powerful. Additionally it may happen that some groups of hacktivists will also publish about cyber attack campaigns on hacking forums or on encrypted chat application groups such as Telegram.

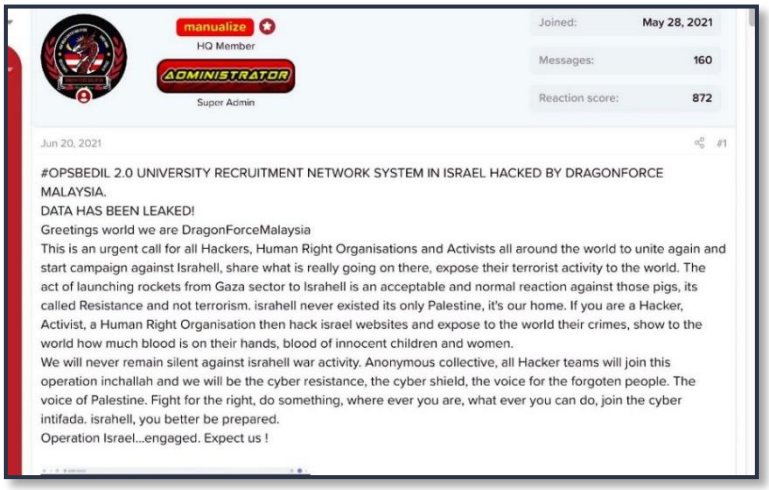


Figure 17: A post annoncing the hack of an Israeli university by the hacktivist group Dragonforce on their forum (source: Dragomforce forum)

Unlike cybercrime, the primary goal of hacktivists is not to make profits. Their main goal is to broadcast an ideology or demonstrate strong opposition to a social, political or religious idea, act or decision taken by a government. There are multiple groups of activists, each with its own pre-vision and ideology. However, many groups join forces for specific campaigns against infrastructures (mostly web) of different countries. When it comes to hacktivism, Cyber HUMINT operations are very useful in collecting confidential information that is not public on social networks. Cyber HUMINT gives the opportunity to infiltrate hacktivist groups in order to identify the targets of cyber attack campaigns as well as to collect information on members of these groups.

Hacktivists often seek to rally as many people as possible to support their cause. It is therefore often easier to infiltrate hacktivist groups with a good fake profile and cover story that allow to gather information from them. In general, to be effective during a Cyber HUMINT operation on hacktivism there are several steps that need to be done including

- The creation of social networks, profiles (fitting to the needs of the operation).
- Joining several social networks public and private groups.
- Being connected to the relevant people (hacktivist members and groups).

6.3 Cyber Terrorism

Cyber terrorism is the use of technological and computer means with the aim of deteriorating or causing permanent damages against the IT systems and critical infrastructures of Nation States. Acts of cyber terrorism are often perpetrated for the purposes of political, ideological, or religious violence. In addition, cyberterrorism aims to sow fear among populations and can therefore be considered as a more aggressive and violent form of hacktivism. Cyber terrorism can also refer to a “cyber enable” threat as some terrorist organizations use the cyberspace (social networks and encrypted messaging applications) as a tool to communicate, promote their ideology and recruit people.

If hacktivism and cyber terrorism have certain similarities, cyberterrorism is generally a bit more offensive. Threat actors seeking to damage national critical infrastructure, recruit people to carry out terrorist attacks or collect intelligence on military operations are often more aggressive than hacktivists. To track and infiltrate some cyber terrorist groups it usually requires several things including a good knowledge of their language as well as a deep understanding of their environment and modus operandi. Cyber terrorists are aware of operational security measures and know how to avoid technological tracking. As for example, a few years ago ISIS had published a user guide on how to avoid security and intelligence agencies' tracking on social networks. They also know how to use encrypted chat applications as well as protecting their devices.

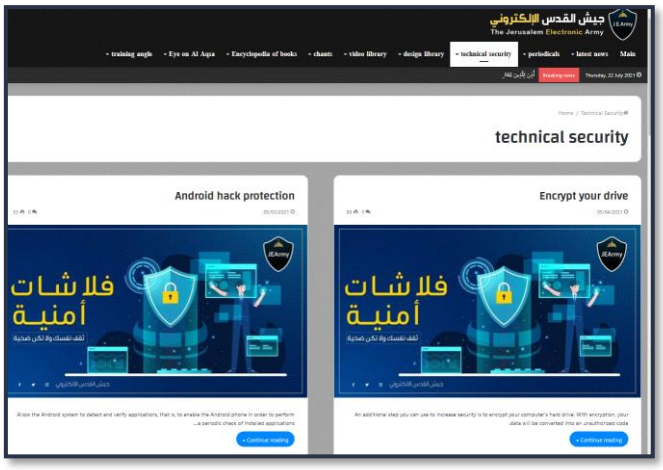


Figure 18: Cyber security guidelines from the Cyber Terrorism group Jerusalem Electronic Army (source: JEArmy website)

One of the Cyber HUMINT modus operandi used by the Hamas to gather intelligence on Israeli military operations and soldiers' geolocation is to create fake attractive young women social network profiles. Once created, they use them to get in touch with Israeli soldiers through messages intended to charm them. These operations aim to infect their smartphone with malware that allows them to collect information on geolocation, messages, emails, and phone conversations. It is often easy to exploit human weakness to implement a Cyber HUMINT strategy that will take advantage of some naivety of targets. The human factor remaining the greatest vulnerability, this technique remains essential and works very often.

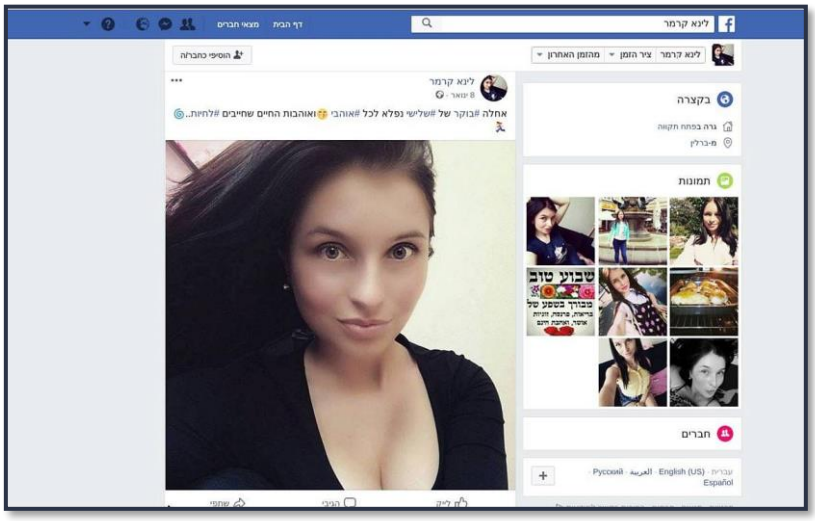


Figure 19: A Facebook profile used by the Hamas to target soldiers with spyware. (source: Times of Israel)

6.4 Cyber Espionage (APT)

Cyber espionage is very relevant to the subject of Cyber HUMINT. In recent years, several Iranian APT groups such as APT34, aka OilRig or APT35 aka Kitten took advantages of the social network Linkedin to carry out cyber HUMINT operations targeting business leaders in the field of high tech, finance and defense. Linkedin is found to be an excellent playground for these APT groups generally linked to governments. It allows them to conduct Cyber HUMINT operations by creating and using fake professional profiles. They virtually approach their targets, build a trusted relation , manipulate and use them as an attack vector.The fact that a large majority of people with various profesionnal backgrounds use social networks such as Linkedin makes it a great way to target them. It allows to contact targets in order to directly or indirectly collect confidential information and / or send malicious links and thus gain a remote access to internal computers and systems.

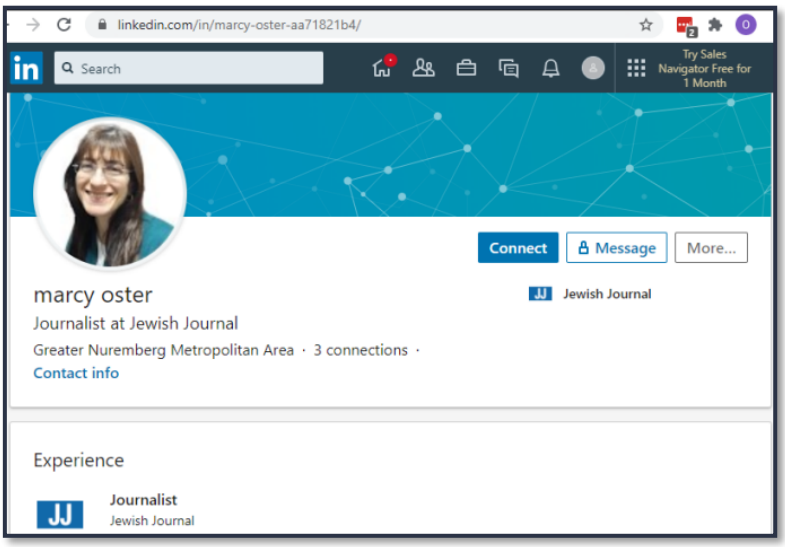


Figure 20: A fake journalist LinkedIn profile created and used by the Iranian APT group Kitten (source: Ban Security Info)

Apart from cyber intelligence campaigns via professional social networks like LinkedIn, some threat actors go further. Firstly, they passively collect information on key people from governments or private companies by using OSINT tools. Secondly, they create real fake corporate email addresses and websites which improve their cover story and credibility. All these elements help them to increase their chances of reaching their targets and gain their trust.

7 Cyber HUMINT: Financial Transactions and Threat Actors Behaviour

Financial transactions are an important element in analyzing the behavior and assessing the skills and security level of threat actors. First of all, it is important to understand that since the emergence of bitcoin and then many other crypto currencies, the behavior of cyber criminals and terrorists toward money has fundamentally changed. If in the past illegal financial transactions had to go through a traditional financial system and obliged threat actors to carry out multiple transactions from accounts to mule accounts coupled with fictitious financial arrangements, it is much easier today for them to carry out illegal transactions in a anonymous and completely secure way outside the traditional financial circuit. Despite some effort on the part of governments to put in place regulatory systems for crypto currencies to avoid illegal transactions and the blaming of dirty money, it is currently very easy to open a bitcoin wallet, buy or sell crypto currencies without any identification process and cash out the money anonymously. The crypto-currency and blockchain systems therefore allow complete anonymization of transactions which makes it a perfect solution for threat actors.

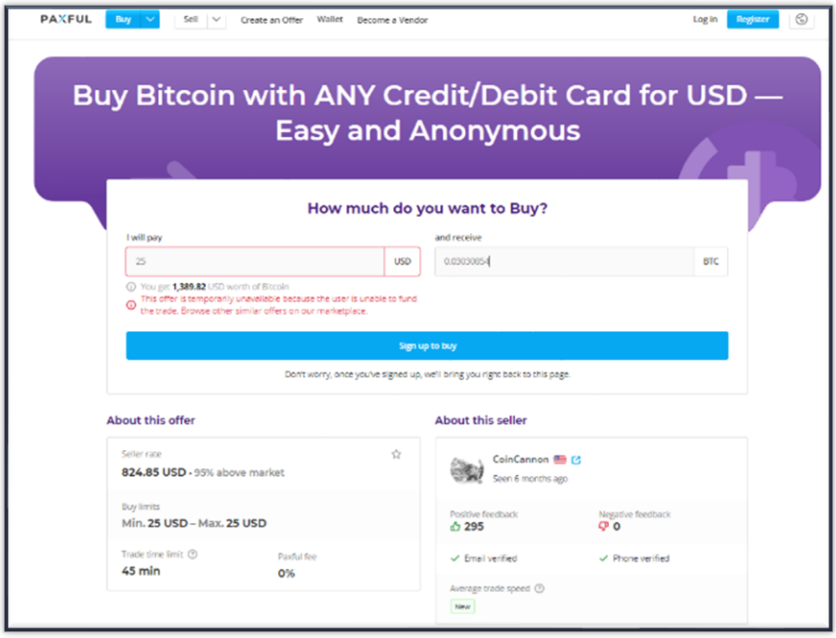


Figure 21: A website that allow to find people who sell and buy bitcoin anonymously. (source: Paxful)

However, the choice of payment method as well as its use allows us to learn a lot about the behavior of the threat actors. According to their geolocation, culture and infrastructure habits, each threat actor will have his preference in terms of crypto currency. Certain threat actors concerned about their security will tend to choose a completely untraceable crypto currency. If transactions carried out in bitcoin and ethereum remain anonymous, they can still be traced on the blockchain. Thus certain threat actors will tend to prefer to use a mixing service. This service allows transfers from one wallet to another, through a multitude of different wallets and sometimes converting the transaction to a different crypto currency on the way. if a threat actor uses a mixing service and chooses especially an untraceable crypto currency, it demonstrates a certain level of operational security.

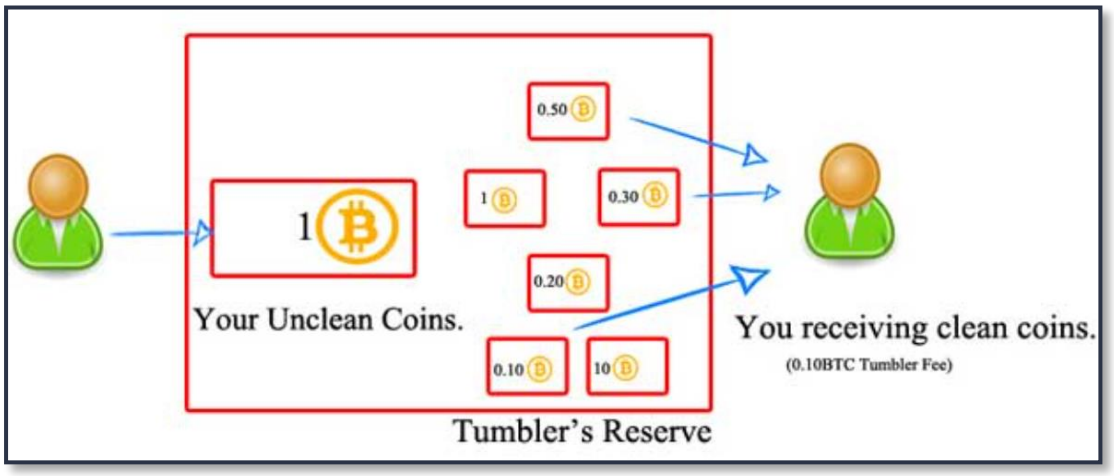


Figure 22: An illustration that explains the principle of Bitcoin mixing (open source)

8 Avatar and Cover Stories

8.1 What is an Avatar?

An avatar or moniker is a fake online virtual identity that allows you to interact with a source or target to gather information about their activities, mode of operation and plans. The creation of an avatar comes with a background story fitting to the environment in which he will be introduced and evolve. Depending on its goal, an avatar can go from a simple email address or nickname to a complete fake cover story and active social network profile with full Personal Identifiable Information (PII), fake pictures, business, and website.

8.2 How to build an Avatar?

Building an avatar requires knowledge and methodology. The success of a Cyber HUMINT collection operation relies primarily on the cover story and behavior of the avatar toward the target. Before creating an avatar, there are a few requirements that need to be respected, including the following:

1. Define the period during which the avatar will be operational (short term/ long term).

2. A deep knowledge of the environment where the avatar will be operating.
   - Cyberterrorism (recruitment methods, culture, ideology).
   - Cyber enabled crime (drug, weapon, human trafficking, child abuse).
   - Cyber-crime (hacking, cyber fraud, crypto money laundering).
   - Hacktivism (cyber-attack campaigns and data leak).
   - Cyber espionage (APT groups structure, Modus Operandi, and attack vectors).

3. Depending on the need of the Cyber HUMINT operation, create a fake profile than can go from a simple email address or nickname to a complete fake profile with:
   - A real fake identity (gender, name, nickname, age, community…).
   - A strong background story (origins, country of living, job and professional skills, family situation...).
   - A fitting profile picture that looks real but that is not (e.g. thispersondoesnotexist.com).
   - A profile on different platforms (social networks, forums, markets, chat applications, email…) according to the needs of the operation.

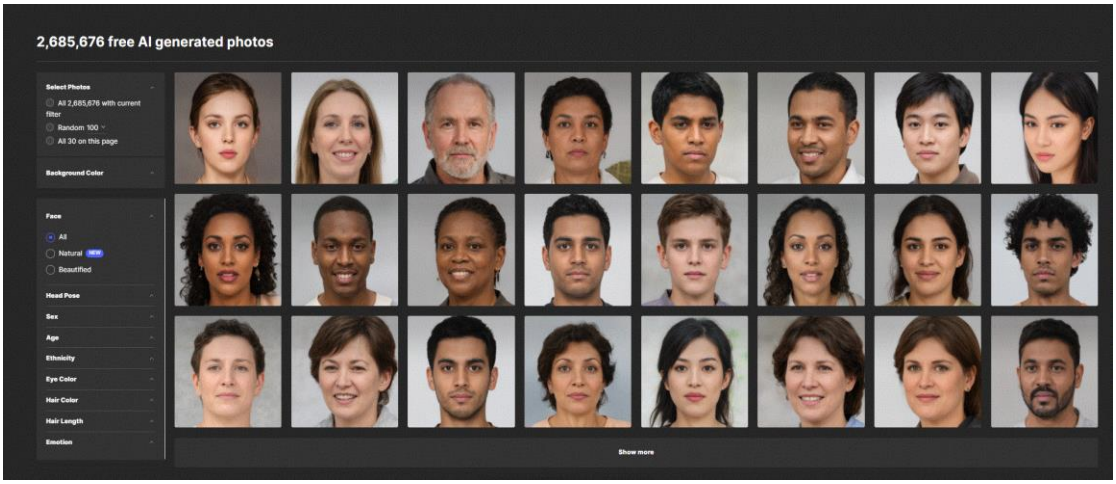


Figure 23: A website to generate non-existent profile photos using artificial intelligence (open source)

Building an avatar is a key step in an undercover operation. When building an avatar, there are certain details that are crucial and should be given special attention. Regarding social networks, it is preferable when creating a fictitious profile to have all the profile parameters that match. Indeed, for example if we create a Facebook profile with a Canadian identity it is preferable to use a Canadian telephone number for its opening and its authentication, to edit the profile with a Canadian city as well as to use a Canadian IP address to have a homogeneous profile.

8.3 Operating and Managing an Avatar

Operating an avatar depends on the environment where it will be operational. Its behavior and activities will be different according to its environment and goal. While each Cyber HUMINT collection operation is unique, there are, however, certain tasks that an avatar should perform to adapt itself to the environment where it operates.

On Forums

- Publish pertinent contents (tutorials, techniques, resources…) as well, as commenting on other members threads at the right frequency (daily, weekly, monthly…) depending on forum's traffic and activities.
- Interact with other forum's members on specific subjects by posting comments or sending private messages.
- Follow and respect forums' rules.
- Build yourself a reputation (in the field you choose).
- Do not republish existing or very similar content.
- Do not use multiple avatars on the same forum (to avoid ban).

When talking about reputation on forums it is important to understand a key point. In the perspective of the implementation of a cyber HUMINT operation especially if it is to be long term, it is preferable to have an avatar with a good reputation but not a great popularity. Law enforcement, intelligence agencies as well as cyber security experts and criminals constantly monitor forums, it is therefore preferable not to have an overly popular avatar who would be too noticeable due to the content he publishes or by his online activities.

On Social Networks

- Publish relevant contents (posts, comments, pictures, videos) at the right frequency depending on the avatar cover story and the goal of the operation.
- Add friends and join communities/groups relevant to the cover story of the avatar (preferably not buying likes and friends as it can look suspicious and is not a reliable technique).

On Encrypted Messaging Applications

- Choose a nickname (preferably letters and numbers instead of names).
- Join and be active in relevant groups/communities (share opinions, ideas, tools, techniques) fitting to the cover story and goal of the operation).
- Do not use the same nickname when interacting with a target that deals with different things in different groups.

9 Cyber HUMINT: Understanding Operational Security (Opsec) Measures

Operational security or Opsec refers to the measures taken to ensure security as well as to remain anonymous on networks. These measures are very important as they provide important indications on the skills level of a threat actor as well as on its techniques . In addition a deep understanding of its measures allows you to better prepare for a Cyber HUMINT collection operation and to protect yourself so as not to reveal sensitive information.

There are several types of opsec configurations but some so-called basic elements are used by many threat actors including:

- Virtual Private Network / Proxy (for anonymous network connection).
- Virtual Private Server (to remain anonymous and store data).
- TOR Browser (for encrypted Darknet and regular browsing).
- Virtual Machine (to protect local computer in case of malware infection).
- Prepaid SIM card (for opening and authentication process of email, social networks and chat applications accounts).
- Encrypted email provider (additionally a PGP key can be used).
- Physically or virtually disable computer's microphone and webcam.

Additionally some threat actors use specific operating system for their opsec such as Linux Tails or Whonix which have a default configuration that uses a TOR browser and automatically encrypts every internet connection. For the past few years cybercriminals and cyber terrorist often use what is called Bulletproof Hosting Service (BPHS) for their operations. This service offers a secure hosting infractructure but with the particularity of not being concerned about the content or the use of the server. They usually pay for this service in crypto currency which makes it even more secure and less traecable. Usually a Bulletproof Hosting service is used by threat actors to perform the following activities:

- To perform spam/phishing (campaigns).
- To use it as a C&C server (to control a botnet of infected machines).
- To drop Exploit Kit.
- To host extremism and terrorism content websites.
- To host hacking and cybercrime forums.
- To host drugs and weapons markets.

10 Advantages and Benefits of Cyber HUMINT

1. Allow to gather intelligence on:
   - Threat actors' profile and motivations.
   - Threat actors' Modus Operandi and TTPs.
   - Technical details and IOCs.

2. Does not require too many investments
   - No need of physical access.
   - No need of complicated and expensive IT infrastructures (mainly open-source tools….).

The only aspect of Cyber HUMINT that could be an issue is the fact that it requires well skilled and experienced people to be engaged in effective online undercover operations. To maximize the chance to perform successful Cyber HUMINT operations, cyber intelligence professionals should have a deep understanding of the world of HUMINT and as well of cyberspace.

11 Cyber HUMINT and Legal Issues

The legal issue is a complex subject. While each country has its own legislation regarding digital activities and the use of personal data, there is often a lack of clear legislation regarding intelligence collection on the web and more specifically regarding Cyber HUMINT operations. There is no international law or regulation regarding Cyber HUMINT activities. It would probably be too complicated to establish rules that would suit all countries. However, from a general perspective, when someone wants to be engaged in Cyber HUMINT activities within a national legal framework, it is important to respect certain rules such as not breaking the law of the country from where the operation is carried out. This usually means not to offer for sale illegal items such as drugs, weapons, fake documents as well as carrying out any form of hacking activities or asking a third party to do so without a legal permission from a State Attorney's Office. Regarding avatars' online activities on criminal forums, it is also important not to post or promote things that violate the law of the country from where the operation is performed. Usually, it is preferable not to post stolen PII or provide malware, exploits as well as hacking tools, and fraud tutorials that could be used by other members. The national legal framework for intelligence services does not generally limit Cyber HUMINT collection operations. Indeed, governments generally allow their intelligence services and militaries to engage in advanced Cyber HUMINT operations under their own national security law. This law, which generally refers to the best interests of the nation and its security, allows the performing of online activities that would not be legal under the traditional national legal framework.

12. Conclusion

While cyber-attack techniques and technologies used by the different types of threat actors are constantly evolving, there is one thing that does not seem to change - the human being behind the keyboard. Indeed, on a yearly base, nation states, institutions and private companies spend billions of dollars on cyber defense and information security systems but forget that the biggest vulnerability is and will remain people. If the human aspect is considered as a vulnerability on the defensive side, on the intelligence one it is a great opportunity. Cyber HUMINT allows performing so-called active intelligence gathering operations that even the best artificial intelligence gathering systems will not allow.

Cyber HUMINT operations allow collecting important and sometimes crucial information about threat actors' capabilities to harm a government, an institution, or a private company. It also gives the opportunity to infiltrate groups of criminals and terrorists for a better understanding of their strategies as well as attempting to identify them and prevent future attacks. However, as previously underlined, Cyber HUMINT operations must be carried out by people with strong professional and technical skills, good knowledge of the human behavior and a good anticipation of the different trends on the various networks. It is not always easy to find competent people with good experience in this area of intelligence. Moreover, the amount of professional training on the market in this domain is still too low in comparison to defensive and offensive cyber security trainings. Cyber HUMINT operations should be more popular with well-defined legal and operational frameworks.

13. About the author

I am a cyber intelligence expert who has worked in a variety of environments over the past 10 years including academia, high tech, military, and law enforcement.

My field of expertise is cyber intelligence including strategy, collection, research, and analysis as well the lead of Cyber HUMINT operations on criminal and terrorist activities within the cyberspace. I have trained many civilian analysts as well as Military and Law Enforcement officers on the Deep & Dark Web environments, Cyber intelligence collection and Cyber HUMINT operations.

14. Thanks

This paper is an operational approach of Cyber HUMINT and reflects a concrete and professional vision. As such, I would like to thank the following people for their advice and support.

- Kobe Schwartz, Head of Cyber Threat Intelligence at Signify
- Ayal Sharon, Superintendent (Ret) Former Head of the Cyber Intelligence Department, National Cyber Crime Unit Lahav 433 Israel National Police and CEO at Tencyber
- Yuval Avargil, Superintendent (Ret) Former Head of the HUMINT Office, National Cyber Crime Unit Lahav 433 Israel National Police.
- Daniel Cohen, Senior Researcher and Lecturer in Cyber Security, at the Yuval Neeman Cyber Research Center from Tel Aviv University, the International Institute for Counter Terrorism from Reichman University and Bar Ilan University

15. References:

1. VINCOS, World Map of Social Networks, January 2021.
   https://vincos.it/world-map-of-social-networks/

2. Link-base, World's biggest link list for hacking & security boards 2021.
   https://link-base.org

3. PORTALFASR, Empire Market.
   https://portalfasr330.weebly.com/empire-market-link.html

4. Bank Security; Cyber Intelligence: HUMINT Operations, June 2021.
   https://bank-security.medium.com/cyber-intelligence-humint-operations-2d3d526e4007

5. MIRCHI9, Shock: ISIS lays trap for youth via WhatsApp, September 2015.
   https://www.mirchi9.com/politics/shock-isis-lays-trap-for-youth-via-whatsapp/

6. XSS.IS, Russian hacking forum.
   https://xss.is/whats-new/

7. DragonForce Forum, Malaysian hacktivist forum.
   https://dragonforce.io/

8. Jerusalem Electronic Army JEArmy, Islamic cyber group.
   https://jearmy.com/

9. Aljyyosh, Hackers armies' forums, the largest Arab forum specialized in new vulnerabilities and hacking sites.
   https://www.aljyyosh.com/vb/

10. Hackforums, The ultimate security technology and social media forum.
    https://hackforums.net/

11. Card Fan Chinese software forum.
    https://bbs.kafan.cn/

12. Times of Israel, Hamas uses fake Facebook friends to dupe 100 soldiers into downloading spyware, July 2018.
    https://www.timesofisrael.com/idf-warns-soldiers-hamas-trying-to-spy-on-them-with-fake-dating-world-cup-apps/

13. Bank Security Info, Iranian Hackers Using LinkedIn, WhatsApp to Target Victims, August 2020.
    https://www.bankinfosecurity.com/iranian-hackers-using-linkedin-whatsapp-to-target-victims-a-14914

14. The Financial Times and Cyberint, Telegram emerges as new dark web for cyber criminals, September 2021.
https://www.ft.com/content/cc3e3854-5f76-4422-a970-9010c3bc732b

15. Generated Photos, Unique, worry-free model photos.
https://generated.photos/