Developing Skills for Open-Source Intelligence Operations

by James Carlini

INTRODUCTION

As discussed in a previous article by this author on MASINT, "Adapting and Adopting Measurement and Signature Intelligence for 21st Century Military Operations," the speed to conduct attacks and counterattacks in war has been greatly accelerated. It has also been extended from the traditional (physical) battlefield into the electronic or cyber battlefields of intelligent infrastructure. This article will explore the need to develop skillsets, understand available software packages, and develop expertise in the area known as OSINT (open-source intelligence).

Like so many other technical and scientific subjects dependent on emerging technologies to support them, new intelligence-based cyber weapons and countermeasures are only as good as the supporting technical devices, sensors, and systems, along with their application by qualified strategists, staff, and technicians. Open-source intelligence is very fast-paced, and ongoing education is imperative and essential to complete the missions engaging this capability.

With these new tools and capabilities, it is critical that the military forces develop expertise across all branches in this area at all skill levels as quickly and expediently as possible. Other functional units which need to interact and interpolate online data, threats, and analytical findings also need to become adept at working with these software-based tools.

OVERVIEW

There is a growing need for cyber specialists who understand the importance of big data analytics in cyberwarfare and asymmetric warfare. America's military needs to invest more in this area as more cyberattacks on both government and private institution targets replace traditional warfare conflicts in doing damage to both the military and the U.S. economy.

OSINT is a broad and dynamic intelligence area which needs a commitment and dedication to constant training because it is expanding rapidly. For its application to be useful within the electronic arsenal of weapons, countermeasures, and cyber systems in a 21st century military, personnel need to be well-trained.

It is a complex function to keep track of, and creatively apply, innovative search technologies for OSINT successfully. In defining OSINT, the U.S. Department of State refers to it as:

> *Open-source intelligence (OSINT) is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.*

As with MASINT, the successful application of OSINT creates a "Collage of Information and Intelligence" from various unrelated sources. A mix of commercial products is available from many different vendors. Security vendors' products go well beyond the typical "Google Search" execution to gather data, utilize it, and create information which then can be used for monitoring and gathering intelligence.

The more capabilities and limitations known about various packages, the more complex an approach for intelligence can be designed and applied to reap a broad and diverse timely perspective on an area of interest. An overview of the packages is included in this article.

WHAT ARE THE IMPORTANT TRENDS?

From an article in February 2022 on AlertMedia's website:

> *Every day, 500 million tweets are published around the world. That's 200 billion posts per year. Add that to the approximately 350 million photos added daily to Facebook, 720,000 hours of new video content added to YouTube every 24 hours, and roughly 500,000 daily Reddit comments, and you start to understand why some say, "The Information Age has become the era of information overload."*

If we are truly in "the era of information overload," the big question becomes: "Out of those 500 million tweets published around the world daily, with a total of over 200,000,000,000 yearly, how many are important; how much of it is garbage; how much more is disinformation; and how much of it is accurate? The same complex question applies as well to all other social media platforms and their vast input of daily information, videos, and pictures posted (see Chart 1).

CHART 1 – PARTIAL LIST OF SOCIAL MEDIA SITES AND DAILY VOLUME OF NEW CONTENT

SOCIAL MEDIA PLATFORM	DAILY VOLUME	TOTAL USERS
TWITTER	500,000,000 tweets	168,000,000 users
YOUTUBE	720,000 hours of videos	210,000,000 viewers in U.S. alone (2022)
FACEBOOK	350,000,000 photos	2,910,000,000 monthly active users (2022)
REDDIT	500,000 comments	26,400,000 users (2022)
ALL of SOCIAL MEDIA	4.5 terabytes of website traffic generated	3,800,000,000 active users

Sifting through all this data needs to be accurate, precise, and most of all fast to gain any type of information and intelligence from the vast quantity of worthless data.

Data has a definite shelf-life or "time limit" on it as far as its value to be found, processed, and analyzed for any shred of usable intelligence advantage. Its value can diminish over time.

Just as milk spoils over time, the value of information found in raw data spoils and decays in terms of its validity for making informed decisions. Hence, we can safely say, "Time is of the essence" when it comes to collecting and analyzing data for any electronic warfare or defensive counterattacks.

When it comes to electronic warfare, infrastructure must be able to sustain unpredicted attack scenarios. As cited in a previous article, "Software-based systems must be resilient and attack-tolerant. The "Five Rs" of mission-critical systems should be adhered to in all important intelligent infrastructure: *Reliability, Redundancy, Robustness, Resiliency, and Resistance-to-Attacks.* These principles should be adhered to in any endeavor developing OSINT-based intelligence systems.

How do you review all that video data? (https://blog.hootsuite.com/how-the-youtube-algorithm-works) As stated in this link, YouTube is as much a search engine as it is a video platform, meaning that a little bit of SEO know-how is important. It is owned by the same company as Google, and some of the search methodologies and tools overlap.

Over the years, YouTube's algorithms have changed. They started with sending a viewer to those videos that were the most popular (see Chart 2). They were bought up by Google in 2006.

CHART 2 – WHAT WAS/IS EMPHASIZED IN YOUTUBE SEARCH ENGINE (its algorithm has evolved)

YEARS	APPROACH USED	COMMENT
2005-2011	Optimizing for clicks & views	Algorithm recommended the videos that attracted the most views or clicks (ClickBait).
2012-2014	Optimizing for watch time	Changed focus to time spent watching each video, as well as time spent on the platform overall. Wanting more viewer feedback to adjust algorithm for more personal preferences.
2015-2016	Optimizing for satisfaction	YouTube measured viewer satisfaction directly with user surveys as well as prioritizing direct response metrics like shares, likes, and dislikes. Came up with white paper on Deep Neural Networks, file:///C:/Users/User/AppData/Local/Temp/45530.pdf.
2016-2021	Dangerous content, demonetization, and brand safety	Moderation of content. Guidelines added for content and search capabilities.
2021-Present	Complex – finding the right video for each viewer & enticing them to keep watching	Algorithm more personalized to search approach, individually focused, also uses external factors to channel searches and their results. More sophistication in both assessing request from user and presenting search results (level of interest, competition, seasonality).

Source: James Carlini, formatting information found at https://blog.hootsuite.com/how-the-youtube-algorithm-works/#A_brief_history_of_the_YouTube_algorithm.

Within the accelerated, sub-second tempo of today's and tomorrow's real-time electronic warfare, and real-time decision frameworks using data, video and information gathered from all types of different sources will be a decisive factor in analyzing situations to allocate resources to win battles and wars in the electronic age.

Here is a summary of the YouTube statistics you need to know (from 2021):

1. YouTube has 2.3 billion users worldwide.
2. 79 percent of Internet users have their own YouTube account.
3. YouTube viewers watch over a billion hours of video on the platform every day and generate billions of views (YouTube, 2021).

4. YouTube is localized in more than 100 countries and is available in 80 languages (YouTube, 2021).
5. Everyday people watch one billion hours of video on YouTube.
6. 62 percent of businesses use YouTube as a channel to post video content.
7. More than 70 percent of YouTube watch time comes from mobile devices.
8. 90 percent of people say they discover new brands or products on YouTube.
9. 400 hours of video are uploaded to YouTube every minute worldwide.
10. 90 percent of U.S. digital video viewers use YouTube, the most popular channel for digital video consumption.

Source: (https://www.oberlo.com/blog/youtube-statistics)

It is also important to highlight that companies like YouTube and Google, which are both owned by the parent company Alphabet, appear to have added some algorithms to skip certain articles and focus you on (steer you to) what they think is important. In other words, it is NOT an objective or all-inclusive search engine process. Filters and other manipulation can be added to their algorithms and information and/or sources can become omitted.

Anyone doing searches needs to know some tools are biased in the way they search, mine, and harvest results. As with the recent COVID-19 searches on YouTube, you are NOT getting ALL the perspectives and that is something which needs to be guarded against, as well as overcome, when conducting OSINT. In some cases, posted videos actually have been taken down and omitted from certain searches altogether.

This was clearly observed when YouTube cut out different perspectives on COVID-19 posted by well-credentialed immunologists. YouTube claims its search process is based on the following key factors but, in addition to this, other filtering algorithms may be engaged:

- **personalization** (the viewer's history and preferences)
- **performance** (the video's success)
- **external factors** (the overall audience or market)

This is something to be aware of. There are alternatives to Google and YouTube when it comes to search engines and, in OSINT, you should be aware of them and their basic capabilities (see Chart 3).

CHART 3 – 20 ALTERNATIVES TO GOOGLE FOR SEARCHING

	SEARCH ENGINE NAME	BRIEF SUMMARY
1	Bing	Microsoft search engine without the YouTube bias on video searches.
2	Brave	Search engine & browser that boasts being three to six times faster than Chrome. Secure. No third-party tracking.
3	Boardreader	Queries its search results from a wide variety of online message boards and forums.
4	CC Search	Search engine for copyright-free content (music, pictures).
5	DuckDuckGo	Privacy on searches. No tracking.
6	Ecosia	Climate change-related. No tracking.
7	Ekoru	No tracking.
8	Giburu	"Preferred Search Engine for Patriots." No tracking.
9	GiveWater	Search engine for poor-quality water and ineffective sanitation.
10	Internet Archive	A vast online library, including old websites, videos, books, etc.
11	Neeva	Ad-free, affiliate-free search engine by former Google engineers. Monthly fee-based.
12	OneSearch	Unbiased, unfiltered search results. No tracking.
13	Search Encrypt	Uses local encryption, Secure Sockets Layer encryption (SSL), to ensure searches remain private.
14	SlideShare	Search engine for documented slideshow presentations, ebooks, & PDFs.
15	StartPage	Google equivalent without tracking of search history.
16	Swisscows	Family-friendly search engine. No tracking and AI-driven.
17	Twitter	Real-time search engine and source of huge range of up-to-

Source: James Carlini, organizing info from https://www.searchenginejournal.com/alternative-search-engines/271409/#close.

NOT ENOUGH RESOURCES? SHOULD WE LOOK TO PMCS?

These electronic (cyber) areas are new in the U.S. military, requiring new skillsets and well-trained personnel. Qualified staff, from technicians to mid-level senior analysts to high-level strategists, are not in abundance across all military branches. Recruiting for these types of positions requires a new selection process focusing on STEM skills as well as other specialized talents.

A question to contemplate is, "Should the American military look at private military companies (PMCs) as a force multiplier for both MASINT and OSINT operations the way the Russians do for traditional asymmetric warfare operations? Should we look at augmenting military intelligence staff with outsiders (contractors)?" (Source: https://publicintelligence.net/awg-russian-private-military-companies/)

There are pro's and con's to answering this question. The pro's are, of course, you have more resources and trained personnel immediately to apply and share the workload, but one of the con's of doing this is that private companies and their personnel are not required to give a sworn commitment as regular military personnel are. Could their allegiance and loyalties be easily compromised? At this point, too many questions need answers if PMCs are to be viewed as a partial solution.

A recent Johns Hopkins Asymmetric Warfare Group research report, "Russian Private Military Companies: Their Use and How to Consider Them in Operations, Competition, and Conflict" (2020), discussed the use of PMCs as force multipliers in more traditional warfare settings. The report did not really ask or answer the question in terms of electronic warfare which should be part of the critical points to cover when doing this type of review at this point in time. Like it or not, every attack and conflict is not at a traditional warfare level or approach.

Electronic warfare is growing, and the recent ransomware attacks are a good example of that growth and the real damage they can cause. The Ukraine conflict is another example in which both traditional and electronic warfare is being waged.

The shortcomings of the Johns Hopkins report are fourfold:

(1) It focuses totally on traditional warfare and traditional warfare logistical issues.
(2) It should include a focus on electronic warfare and cyberattacks (this is something which should be thoroughly reviewed by the research team as warfare shifts more from traditional to electronic (cyber) attacks including ransomware and other denial-of-service viruses).
(3) The report is focused on Army-related concerns only and not on overall (multi-branch) concerns. (When it comes to cyberwarfare an underused "force multiplier" may be the use of inter-branch expertise. The Army helps other branches and vice versa depending on needs and demands. Combined inter-branch action can be an alternative force multiplier.)
(4) It keeps the leadership focus on preparing and "fighting the last war" (Blitzkrieg- style traditional warfare), instead of preparing for the next war (NANOKRIEG—cyberwarfare, cyberattacks on infrastructure and data centers, as well as other electronic threats, such as EMP).

In developing cyber expertise quickly, it is better to pool all branches of the military together for training. We should avoid the separate approaches used with so many other traditional military training endeavors in which the outcome is "this is the way we do it in the Navy" or "these are standard Army procedures" (see Chart 4A).

We need to develop and cross-train skillsets so that all branches can share and utilize the combined expertise and perspectives of specialists and strategists, as well as the institutional insights gathered through electronic warfare and cyberattacks across all branches.

Compared to developing traditional "branch-specific" warfare skillsets (identified by Green in Chart 4A), which take much longer to cultivate and execute on a single-branch basis, this would be a more effective approach. Branch-specific training may be an advanced course or a future add-on. Today, we need as many trained people across all branches as quickly and expediently as possible.

Training approaches should reflect getting ALL branches up to speed as quickly as possible and then creating specialized and advanced courses that would be more branch-specific (see Chart4B).

CHART 4A – TRADITIONAL "DO IT OUR WAY" BRANCH APPROACH TRAINING

ARMY	NAVY	AIR FORCE	SPACE FORCE	COAST GUARD	MARINES
COURSE 1 INTRO	COURSE 1 INTRO	COURSE 1 INTRO	COURSE 1 INTRO	COURSE 1 INTRO	COURSE 1 INTRO
COURSE 2	COURSE 2	COURSE 2	COURSE 2	COURSE 2	COURSE 2

Source: James Carlini.

CHART 4B – ALL-BRANCH APPROACH TRAINING WITH SPECIFIC COURSES AFTER INITIAL FIRST THREE

COURSES	ALL BRANCHES
1	INTRODUCTION
2	INTERMEDIATE SKILLS
3	ADVANCED SKILLS (Qualified)
4	BRANCH-SPECIFIC SKILLS

Source: James Carlini.

Chart 4B reflects a faster ramping-up of skillsets, getting as many analysts as possible trained, and then, later, focusing them on more advanced, branch-specific areas of importance (green area).

GOOGLE ADVANCED SEARCH CAPABILITIES FOR OSINT

Google is a commonly used search engine which can also provide a more detailed and comprehensive search than what most people use it for in everyday searches. It could be used for some OSINT applications and should be analyzed as to what role it plays in OSINT.

Advanced search operators from GOOGLE include the following operators. It is referred to as Google Dorking (see Chart 5). The term "Google Dorking" describes the more intense and advanced search capabilities using the Google Engine and the above operators to obtain more specific intelligence across a wider breath of online sources. There are also other commercially available packages like Authentic8 and Mandiant, providing OSINT capabilities and SEO (Search Engine Optimizations).

There are resources which can be accessed to obtain information and techniques used by cyberterrorists which should also be learned as a basic foundation for OSINT techniques and countermeasures beyond Google. One of those sources is PublicIntelligence.net, which has many insights to skillsets and information needed by those in the media as well as terrorists and counterterrorists who tend to utilize any tool which is readily available to them. Remember, some tools are free and do not need a subscription or other fee paid for access. Public Intelligence's mission is described as:

> *Public Intelligence is an international, collaborative research project aimed at aggregating the collective work of independent researchers around the globe who wish to defend the public's right to access information. We operate upon a single maxim: equal access to information is a human right. We believe that limits to the average citizen's ability to access information have created information asymmetries which*

CHART 5 – GOOGLE ADVANCED SEARCH OPERATIONS (with Various Operators)

OPERATOR	ACTION
allintext: /intext:	Restricts results to those containing all the query terms you specify in the text of the page.
allintitle: /intitle:	Restricts results to those containing all the query terms you specify in the title.
allinurl: /inurl:	Restricts results to those containing all the query terms you specify in the URL.
filetype: suffix	Limits results to pages whose names end in *suffix*.
site:	Using the *site*: operator restricts your search results to the site or domain you specify.
Minus sign (–) to exclude	Placing a minus sign immediately before a word indicates you do not want pages containing this word to appear in your results.
Phrase search (using double quotes, "…")	By putting double quotes around a set of words, you are telling Google to consider the exact words in that exact order without any change.

Source: (https://publicintelligence.net/dhs-fbi-nctc-google-dorking/).

threaten to destabilize democratic rule around the world. Through the control of information, governments, religions, corporations, and a select group of individuals have been able to manipulate public perception into accepting coercive agendas which are ultimately designed to limit the sovereignty and freedom of populations worldwide.

There are more special operators which can be used for searching and they are described here: https://ahrefs.com/blog/google-advanced-search-operators/.

The use of the ShowmyIP.com is a start in understanding what is revealed and what to look for in an IP address (Internet Protocol) for OSINT research (https://www.showmyip.com/). For example, when you go to the website, your IP address will appear: 107.219.121.249. Each user needs to have an IP address in order to use the Internet (see Chart 6).

All these tools can help investigate ownership and hosting information about the sites relevant to your research. Using WHOIS records and advanced search engine techniques can reveal identifying details about the host, moderator, and IP, as well as what other sites might be sourced from the same owners.

That number translates to all this location and vendor information about where it is originating.

CHART 6 – SAMPLE IP ADDRESS AND INFORMATION

IP ELEMENT	INFORMATION
Your IPv4	107.219.121.249
Your IPv6	2600:1700:3090:2eb0:89a2:97a1:be72:7ba5
Country	United States
Region	Illinois
City	Gilberts
ZIP	60136
Time zone	America/Chicago
Internet Service Provider (ISP)	AT&T Services, Inc.
Organization	AT&T Corp.
AS number and name	AS7018 AT&T Services, Inc.
User agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0); Gecko/20100101; Firefox/89.0

COMMERCIAL AVAILABLE PACKAGES THAT SHOULD BE REVIEWED

Authentic8, FireEye (Mandiant), and other packages are available to both commercial and government agencies for threat intelligence capabilities used in OSINT applications. The full field of significant companies providing some type of threat intelligence/cyberattack review services includes: CrowdStrike, Digital Shadows, FireEye, Flashpoint, Group-IB, IBM, Intel 471, IntSights, Kaspersky, Recorded Future, RiskIQ, and ZeroFOX.

No one tool can review all aspects within OSINT. Hence, there is be a mix of tools that analysts and strategists would use. Some general descriptions of OSINT are provided in Charts 7A and 7B.

CHART 7A – NETWORK ADMINISTRATOR USING OSINT

MAIN REASONS FOR USING OSINT	DESCRIPTION
PENETRATION TESTING	Gather all the information that is available out there and see if any of it can lead to an indication that your network has been compromised.
BREACH DETECTION	Monitoring the Internet using OSINT could give you an early start in damage control and even catch the people behind the data theft. Alternatively, it could simply be that a public-facing (or peripheral) device has not been secured well enough and could be leaking data.
ETHICAL HACKING	Turn the table and gather information on a source-target; find out everything you can about competitors/threats and use it to gain an insight into their way of doing things.
CHATTER MONITORING	Monitor traffic and packets to see what is being directed your way; use the tools to find out all you can before an attack occurs.

Source: https://www.comparitech.com/net-admin/osint-tools/.

Some OSINT tools on the market have all three functionalities (Discovery, Scraping, and Aggregation) included in one package. There are three methods of OSINT intelligence gathering: Passive, Semi-Passive, and Active, as shown in Chart 8.

In any OSINT operation, it is always safe to assume the target(s) will detect and uncover the intelligence probe. Chances are, they will execute some countermeasures and even a counterattack. Therefore, the use of fake accounts, private VPNs, and other masking tools and tactics is necessary and should be learned as part of the basic OSINT skillsets and tool kits.

Countermeasures to all this searching and probing are growing as more organizations install obstacles to block surveillance and penetration (https://traversals.com/blog/osint-investigations/). This is why the area has to be viewed as one which requires continual specialized education in order to keep up with changes and new, dynamic approaches within surveillance techniques.

CHART 7B – THE THREE MAIN CATEGORIES OF OSINT TOOLS

TYPE OF TOOL	DESCRIPTION
DISCOVERY	Used to search for the information that is out there. A great example would be Google. Besides simple searches, Google has advanced search capabilities as shown in Chart 1.
SCRAPING	Once discovered, the data must be "scraped" and collected somewhere safe. These tools make sure only the required data is filtered for extraction to avoid bulky transfers (which could alert the source).
AGGREGATION	Once the data has been stored safely, it needs to be mined and sifted through to convert it into usable information. These tools are used to combine related data bits into a larger picture, present it in a way showing relations and connections between datasets, and consolidate it in a consumable format.

CHART 8 – THREE METHODS OF INTELLIGENCE GATHERING IN OSINT

INTELLIGENCE GATHERING TYPE	APPROACH
PASSIVE	"Normal" way of digging for information; usually done by scouring the web with applications like Google search, Bing Maps, and Yandex images. Hard to detect as no probing is involved.
SEMI-PASSIVE	Scouring the Internet is involved to find the data, but software solutions are also involved to gather information about a network non-intrusively. No brute force attack or in-depth querying is involved.
ACTIVE	The information is collected by directly extracting it from the target, though no malicious software is involved in breaching the security. This type of probing can be detected because it involves scanning of networks to find open ports, for example. Could be perceived as hacking.

CHART 9A – THE PRO'S AND CON'S OF OSINT

PRO'S	DESCRIPTION
COST-EFFECTIVE	Good if budgets are not large, and you do not have a lot of money for tools and specialized packages.
GOOD RETURN ON INVESTMENT	If you do buy a tool, they are usually effective for gathering info.
OPEN & ACCESSIBLE SOURCES	You do not need a lot of "special packages"; consequently, you do not need a lot of specialized training.
SPEEDS UP THE ANALYSIS OF THREATS & DECISION-MAKING	Addresses both strategic and tactical areas.

Source: https://www.comparitech.com/net-admin/osint-tools/.

CHART 9B: OSINT DISADVANTAGES

CON'S	DESCRIPTION
DELUGE OF INFORMATION	You must sift through all of it to get to the important parts of what you are looking for.
TIME-CONSUMING	If you are looking for something specific, you will need some tool to narrow down your focus.
NOT READY-TO-USE, UNLESS YOU HAVE A TOOL	You need to invest in some type of package or packages.

When it comes to cybersecurity, major players and start-up companies are acquiring more and more skills and tools to keep up with the competition (see Chart 10). There is also some consolidation going on as far as companies acquiring some of their competition.

If OSINT is to be a key foundation for military intelligence in the 21st century, having good skillsets in systems and software tools is critical for all personnel assigned to this area. This is a very broad area with a diverse and growing set of complex tools. All branches of the military need to ramp up training and courses if they want to develop a cadre of personnel at all levels of expertise and decision-making skills in this area.

Big data, sprawling across so many different detail-rich database platforms representing credit information like banking, cryptocurrencies, spending patterns, as well as social network interactions from family and friends to business connections, need to be covered within a surveillance umbrella of Total Information Awareness (TIA)

CHART 10 – TEN MOST POWERFUL CYBERSECURITY COMPANIES

COMPANY	RECENT ACQUISITIONS	WHERE THEY ARE IN THE MARKETPLACE
CISCO	Cisco bought Kenna Security in May 2021, which provides risk-based vulnerability management technology.	Cisco as a visionary in its endpoint protection rankings. Gartner notes Cisco's SecureX cloud-based service integrates security analytics, threat hunting, and threat intelligence in a single view.
CLOUDFLARE	Purchased S2 Systems, a Seattle-area startup with a unique innovative remote browser isolation solution.	Built out one of the largest global content delivery networks and became a leader in cloud security.
CROWDSTRIKE HOLDINGS	CrowdStrike acquired Preempt Security, a provider of zero-trust and conditional access technology for threat prevention, and Humio, a provider of high-performance cloud log management technology.	CrowdStrike has emerged as a leader with its Falcon platform and "has a strong reputation as the single solution for organizations looking to consolidate their endpoint protection and endpoint disaster recovery solutions," according to Gartner.
FORTINET	Bought cloud-based IT operations management vendor Panopta. In March 2021, Fortinet bought network security vendor ShieldX and in July it bought continuous AppSec testing vendor Sken.ai.	
IBM	In January 2021, IBM acquired StackRox, a provider of container and Kubernetes-native security software.	IBM is a leader in enterprise-grade security. IBM's security portfolio includes the industry leading QRadar SIEM.
MANDIANT (soon to be part of Google)	Divorced itself from FireEye and is now a stand-alone company bought out by Alphabet, Inc. (Google).	Expanded its offerings beyond consulting to include SaaS-based security validation, threat intelligence, and managed detection and response.

Source: Chart information from https://www.csoonline.com/article/3531668/the-10-most-powerful-cybersecurity-companies.html?page=2).

and be available to review, assess, and analyze. We should also look at what is on the horizon regarding new platforms.

METAVERSE: A CYBER-SANDBOX FOR TERRORISTS?

When it comes to electronic warfare, we must also include understanding the impact of the next "big thing" appearing on the horizon: Metaverse. As mentioned in a recent article for the National League of Cities:

> *It's an online space that digitally recreates the real world. For others, it is a shift in how people interact with their world, using technologies like 3D computing, augmented reality, virtual reality, and blockchain to form new immersive virtual world experiences.*

Metaverse incorporates Artificial Intelligence (AI), Virtual Reality (VR), and other "Augmented Reality" (AR) software to create a whole new platform for information gathering, communications, and counterintelligence. This emerging platform already has some real applications that have been developed and are broken down into their key aspects (see Chart 11 below).

Does it have any significant military intelligence value? I believe it has. At a minimum, it should be understood as well as analyzed in terms of having benefits or hidden vulnerabilities which can be exploited in a cyberwarfare event. Because Metaverse does have the ability to manipulate cryptocurrency platforms, I believe the safe bet would be to include it in any study of OSINT or any other aspect of electronic warfare or cybercrime in which financial ransomware and other malware can be activated.

As a by-product of the pandemic lockdown, Facebook CEO Mark Zuckerberg explained his perspective that the "metaverse" spans non-immersive platforms like today's social media as well as immersive 3D media technologies such as virtual reality, and that it will be applicable as a virtual "work zone" as well as for play in the near future. Because of its future capabilities and proposed interactions with cryptocurrency platforms, now is the time to include it in any study of sources for future intelligence gathering and monitoring of operations on the Internet.

In a very recent article, some cities are already looking at applications of Metaverse for everyday operations. In its article on utilizing the Metaverse in cities, the NLC focuses on this application:

> *The integration of GPS with public transit means that riders now take for granted the ability to perfectly predict the moment their bus will arrive, and access to broadband has enabled residents to reliably connect to their jobs, schools or loved ones from their homes.*

Would not this also be the perfect tool to plan for detonating explosives on the same bus route? Access to this specific a schedule could be the blueprint for a terrorist cell to take out a group of people or a specific rider who it knows will take a specific bus every day.

This new platform should be analyzed as to what military value it may have and what security vulnerabilities it creates in both traditional and electronic data gathering. Anything put on a Metaverse platform should have security safeguards on it, but that is something I am certain has not been thoroughly thought through. Where is the "Framework (guidelines) for Security"?

CHART 11 – THE KEY ASPECTS OF METAVERSE

	KEY ASPECT	DESCRIPTION
1	PRESENCE	A sense of presence is achieved through virtual reality technologies.
2A	INTEROPERABILITY	Ability to travel seamlessly between virtual spaces with the same virtual assets, such as avatars and digital items.
2B	INTEROPERABILITY (TRANSFER OF DIGITAL GOODS ACROSS VIRTUAL BORDERS)	Exchange of cryptocurrencies, nonfungible tokens (NFTs) (I broke this into a separate section as I believe it should be distinct).
3	STANDARDIZATION	Interoperability of platforms and services across the metaverse. Open Metaverse Interoperability Group (Standards Group).

Source: James Carlini.

The way it appears today, Metaverse could be the virtual platform that supports a "cyber-sandbox" to plot, test, and further refine terrorist attacks on whatever is represented on a Metaverse platform before an actual attack is initiated. Consequently, all the work a city does to create an accurate virtual image of itself will also give terrorists a crystal-clear blueprint outlining its vulnerabilities and security soft points.

CHART 12 – APPLYING METAVERSE TO ASYMMETRICAL WARFARE

AREA FOCUS	DESCRIPTION
REMOTE WORK EXPERIENCE	Have teams working together virtually, while in reality they are remote and not together (coordination of terrorist cells).
RECRUITMENT OF PERSONNEL	Metaverse offers a platform to connect with other people virtually (recruiting for extremist groups, spreading ideology of groups).
ASSESSMENT OF WHAT TO ATTACK?	Diagrams, blueprints, and other schematic diagrams could be obtained. Detailed descriptions of infrastructures and other logistical information.
COORDINATION OF THAT ATTACK	Getting all the elements together for some guerrilla attack or overtaking an area.
CRYPTOCURRENCY	Since cryptocurrency is also in the plans for metaverse applications, cybercrimes which are already a big part of this financial area will continue to evolve and expand. This area alone should dictate that Metaverse be covered in intelligence monitoring and surveillance.

Source: James Carlini

This entire new area of concern should be a wake-up call for stronger security measures and perhaps a step back as to what information is put out to the public.

The exchange of NFTs (Non-Fungible Tokens) is another area of concern which has elements of legitimacy within it, but can be another huge playground for fraud, ransomware, and other criminal activities. It is anchored in blockchain technology, but that does not make it totally impermeable to fraud and counterfeiting.

What is an NFT? In a recent *Forbes* article, the author describes an NFT as being created, or "minted," from digital objects representing both tangible and intangible items, such as:

- *Graphic art*
- *GIFs*
- *Collectibles*
- *Videos clips and sports highlights*
- *Virtual avatars and video game skins*
- *Designer sneakers*
- *Music*

> *Even tweets count. Twitter co-founder Jack Dorsey sold his first ever tweet as an NFT for over $2.9 million.*
> *Essentially, NFTs are like a physical collector's items, only digital. Thus, instead of getting an actual oil painting to hang on the wall, the buyer gets a digital file instead.*

NFTs can be the equivalent to Digital Beanie Babies. Get yours NOW and watch their values explode—until they do not!

There are more and more con's coming out. Their "value" is a real pseudo-value that gets hyped and "certified" by a couple of wild transactions to get your attention and confidence. "Oh, it is a legit digital marketplace, backed up by blockchain technology." This entices you to invest your money in it, and then see your money evaporate into the ether. Biometric safety measures have also been compromised. In a recent report, this was revealed:

> *The 2021 Identity Fraud Report from Veriff shows a 61 percent increase in fraudulent activity in the fintech, mobility and crypto industries from 2020 to 2021.*

Are there some "legit" transactions? SURE, but the whole process seems much too easy to create a lot of scams and black holes where your money gets "lost" or, worse yet, unable to be accessed because the "key doesn't work anymore" into the digital wallet.

Remember, blockchain technology was hyped as being very secure in the cryptocurrency arena. Yet, criminals managed to find billions of dollars of scams and criminal capabilities within it. The same criminal element will look into applications of Metaverse and find other vulnerabilities to exploit for criminal gain.

When it comes to targets in electronic warfare, nothing is off-limits. There has been no attempt to create a Geneva Convention for cyberwarfare operations and the reality is there probably never will be. No digital platform has been ruled exempt or off-limits when it comes to cyberattacks, fraud, theft, and destruction.

[Author's Note: This article is an excerpt from my upcoming book titled *Nanokrieg: Beyond Blitzkrieg*, which explores strategies needed to fight the War on Terrorism as well as any non-traditional asymmetric warfare conflict in the 21st century.]

References

OSINT
What Businesses Need to Know About Open Source Intelligence (OSINT)
https://www.alertmedia.com/blog/open-source-intelligence/

How Does the YouTube Algorithm Work in 2021? The Complete Guide
https://blog.hootsuite.com/how-the-youtube-algorithm-works

10 YouTube Stats Every Marketer Should Know in 2021 [Infographic]
https://www.oberlo.com/blog/youtube-statistics

20 Great Search Engines You Can Use Instead of Google
https://www.searchenginejournal.com/alternative-search-engines/271409/#close

Asymmetric Warfare Group Study: Russian Private Military Companies in Operations, Competition, and Conflict
https://publicintelligence.net/awg-russian-private-military-companies/

DHS-FBI-NCTC Bulletin: Malicious Cyber Actors Use Advanced Search Techniques
https://publicintelligence.net/dhs-fbi-nctc-google-dorking/

Google Search Operators: The Complete List (42 Advanced Operators)
https://ahrefs.com/blog/google-advanced-search-operators/

What Is My IP?
https://www.showmyip.com/

5 Ways to Protect Your OSINT Investigations
https://traversals.com/blog/osint-investigations/

The 8 Best OSINT Tools
https://www.comparitech.com/net-admin/osint-tools/

The 10 Most Powerful Cybersecurity Companies
https://www.csoonline.com/article/3531668/the-10-most-powerful-cybersecurity-companies.html?page=2

From Our Partners – Nanokrieg Beyond Blitzkrieg: Mindset to Fight the War on Terrorism,
by James Carlini
https://cip.gmu.edu/2015/09/21/from-our-partners-nanokrieg-beyond-blitzkrieg-mindset-to-fight-the-war-on-terrorism-by-james-carlini/

Metaverse

What Is the Metaverse? 2 Media and Information Experts Explain
https://theconversation.com/what-is-the-metaverse-2-media-and-information-experts-explain-165731

Cities and the Metaverse
https://www.nlc.org/resource/cities-and-the-metaverse

How Cities Are Engaging in the Metaverse
https://www.nlc.org/article/2022/04/18/how-cities-are-engaging-in-the-metaverse/

Open Operability Standards Group
https://www.w3.org/community/metaverse-interop/

The Metaverse Offers a Future Full of Potential – for Terrorists and Extremists, Too
https://www.nextgov.com/ideas/2022/01/metaverse-offers-future-full-potential-terrorists-and-extremists-too/360494/

Get Ready for the Metaverse
https://gcn.com/emerging-tech/2022/04/get-ready-metaverse/366029/

Streetlights Leverage Digital Infrastructure for Smart City Apps
https://gcn.com/emerging-tech/2022/04/streetlights-leverage-digital-infrastructure-smart-city-apps/365752/

I've Seen the Metaverse – and I Don't Want It
https://www.theguardian.com/games/2022/jan/25/ive-seen-the-metaverse-and-i-dont-want-it

What Is an NFT? Non-Fungible Tokens Explained
https://www.forbes.com/advisor/investing/cryptocurrency/nft-non-fungible-token/

Geneva Convention in Cyberwarfare? Don't Count on It
https://intpolicydigest.org/geneva-convention-cyberwarfare-don-t-count/

Europol Finds Urgent Actions Needed to Counter Criminals Using Deepfakes
https://www.biometricupdate.com/202204/europol-finds-urgent-actions-needed-to-counter-criminals-using-deepfakes

James Carlini is a visionary and strategist for mission-critical networks, technology, and intelligent infrastructure. He has been president of his own consulting and research firm since 1986. He is the author of LOCATION LOCATION CONNECTIVITY: Next-Generation Real Estate, Intelligent Infrastructure, Technology, and the Global Platform for Commerce *(published in 2014). Holding an MBA degree, he is a former award-winning adjunct faculty member at Northwestern University in both the executive master's and undergraduate programs (1986-2006), developing and teaching courses in strategic technology management, team dynamics, Lean Six Sigma, network security, and international applications of technology. He also has served as an expert witness in civil and federal court trials on mission-critical networks and intelligent infrastructure. His original "Platform for Commerce" definition of infrastructure and its impact on economic growth was written in a 2009 white paper for the U.S. Department of Homeland Security, titled "Intelligent Infrastructure," and was later adopted and referred to in a U.S. Army Corps of Engineers handbook*, Infrastructure and the Operational Art *(2014), and its 2016 publication* Infrastructure in Subpopulations. *Jim has written frequently for* AIJ *in the past. He served in the Air National Guard and the U.S. Army Reserve from 1972 to 1985.*