DARKOWL

NATION-STATE ACTORS ON THE DARK WEB

EXAMINING HOW NATION-STATES USE THE DARK WEB, AND HOW THE AVAILABILITY OF NEW TOOLS HAS LEVELED THE GLOBAL PLAYING FIELD OF CYBER CAPABILITIES

INTRODUCTION

One defining characteristic of the dark web is its association with criminal activity, where it is most often known as a haven for drug and gun dealers, hackers, pornographers, scam artists and other criminals. But this stereotype may at times be oversimplified. While there are some objectively clear cut parameters of criminality, there also is a gray area comprised of politically motivated operatives who may or may not be committing crimes as commonly defined, but are nevertheless acting to influence and further an agenda of their own making. These groups, including Nation-State Actors – state-sponsored hackers with a cyber warfare mission – are worth examining in their own right.

WHY NATION-STATES TURN TO THE DARK WEB

The dark web provides an anonymous environment in which anyone can operate. Of importance and relevance to Nation-States, a number of key objectives can be carried out under this cloak of anonymity. Nation-State cyber actors will utilize the dark web to conduct intelligence collection and source development, government and corporate espionage, exploit development and testing, disinformation operations for geopolitical influence, infrastructure disruption, and financial gain.

TABLE OF CONTENTS

Why Nation-States turn to the dark web (cont.)

Intelligence and Espionage

The early beginnings of cyber-based information operations were conducted by the US government's National Security Agency (NSA) and China's People's Liberation Army (PLA). While the NSA used information operations for covert intelligence collection from foreign adversaries, China is well known for its extensive espionage and intellectual property theft activities with much success. This includes surveillance of its own citizens and their use of the dark web to attempt to circumvent state controls.

Profitability

Countries facing extreme US and UN economic sanctions are turning to the dark web for financial gain. In recent years, North Korea has been successful in launching nation-wide banking system hacks across east Asia.

Exploit Acquisition and Development

Many blackhat exploits are discussed in dark web forums and encrypted chats, as frequently observed on DarkOwl Vision. System vulnerabilities are detailed and shared for all types of critical operating systems and unix distributions. The dark web provides a valuable resource for researching and testing source code anonymously.

Activism and Propaganda

Whether it is religious differences in the Middle East or ideological differences in the South China Sea, political activism and propaganda have been an effective weapon of Nation-States for decades. Given society's shift to persistent digital communications, cyber has become a preferred medium for this type of activity. Nation-States, both large and small, have used cyber activity to do everything from promoting their agendas, to propping up proxy states both in the dark web and across social media platforms.

Infrastructure Disruption

Nation-State-funded cyber campaigns against other Nation-States has become wide-spread, principally targeting networks containing sensitive government or corporate information and strategic plans. In late 2015, Russia demonstrated how kinetic attacks conducted against critical infrastructure (e.g., telecommunications, utilities, etc.) and information outlets could cripple a Nation-State, with hacks against Ukraine during on-going conflicts over Crimea. Additional cyber-based attempts to infiltrate key US utilities infrastructure has been detected and reported by the US Department of Homeland Security and multiple cybersecurity

Background on global cyber warfare climate

Modern cyber warfare has a much older pedigree than one would suspect originating from influence warfare and propaganda campaigns during WW1. Information Operations and Influence Warfare is a concept used widely since the world wars where Americans and the British effectively used propaganda to influence attitudes around the world. Influence warfare has been used ever since both covertly and overtly to influence geo-political events and populations. A most recent example is Russia's troll farm setup by the Internet Research Agency to influence US citizens during the 2016 Presidential election. Information Operations in the digital sphere has been well-formulated and established by the US government in military field manuals and standard operating procedures.

ANALYSIS: ESTIMATING THE MOST POWERFUL NATION-STATE ACTORS ON THE DARK WEB BY COUNTRY

The making of a cyber superpower: Money, Manpower, Skill and Influence

DarkOwl has undertaken an estimation of the relative power of Nation-States in the darknet, along the axis defined in Image A (below). Of the four variables used by our analysts to determine the extent of a Nation-State's cyber power — Money, International Influence, Manpower and Skill — the US, Russia and China lead in all four categories. All three countries have significant capital at their disposal, as well as the academic infrastructure backing cyber related research and a formidable presence on the economic world stage.

Evaluating an additional 16 key Nation-States against these same four variables provides insight into their presence on the dark web and preferential use of cyber as a weapon. However, the release of cyber tools previously belonging exclusively to the NSA and the CIA have offered formerly less-powerful nations the ability to reframe themselves as power players and gain influence that was previously unattainable to them.

SEE PAGE 12 FOR THE FULL LIST & ANALYSIS OF COUNTRIES, RANKED BY CYBER INFLUENCE

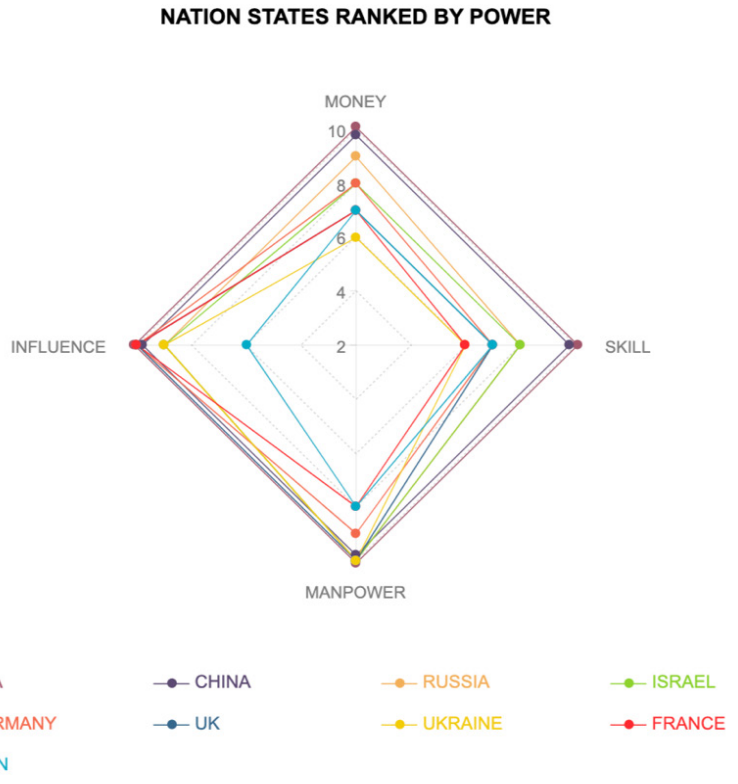

Image A - Graphic depicting the top Nation States as determined by the extent of their cyber influence

A CHANGING LANDSCAPE: A LOOK AT THE NEW TOOLS THAT NATION-STATES ARE USING ON THE DARK WEB

Shadow Brokers & the release of Vault 7/8

In the summer of 2016, the mysterious hacking group Shadow Brokers began releasing multiple sets of "ops disks" (toolkits) used by the US National Security Agency that they had nefariously collected using persistent access since 2013. The unprecedented data gave insight into the inner workings of the most sophisticated hacking organization in the world, NSA's Tailored Access Operations (TAO). The disks included UNITEDRAKE's "fully extensible remote collection system" also mentioned in data released by Edward Snowden, the NSA whistleblower still in exile in Russia. Pronounced "United Rake," this customizable malware supports espionage and mass surveillance with such abilities as capturing IP camera and microphone output, log keyboard input, access external drive data. This toolset also provides the unique capability to disguise the origin of the attack, effectively projecting attribution onto another country or hacking group.

Wikileaks followed shortly thereafter with releases of CIA's infamous Vault 7 and 8, which included one of the largest collection of confidential documents to ever slip out of the CIA. The Vault 7 release discussed the Remote Device Branch's project UMBRAGE group sophisticated false flag operations as well Weeping Angel, where IoT devices, such as smart televisions are exploited for use as spyware.

The most notable leak from the CIA Vault 8 was HIVE, a multi-platform CIA malware suite with its associated control software. The project provides hidden customizable "implants" for Windows, MikroTik (used in internet routers), Sun Solaris, and Linux platforms. HIVE also included a comprehensive Listening Post (LP) and Command and Control (C2) infrastructure to communicate with these implants that have been extensively studied and now in the arsenal of various international hacking groups of all skill levels ranging from amateur script kiddies to advanced cyber Nation-State Actors.

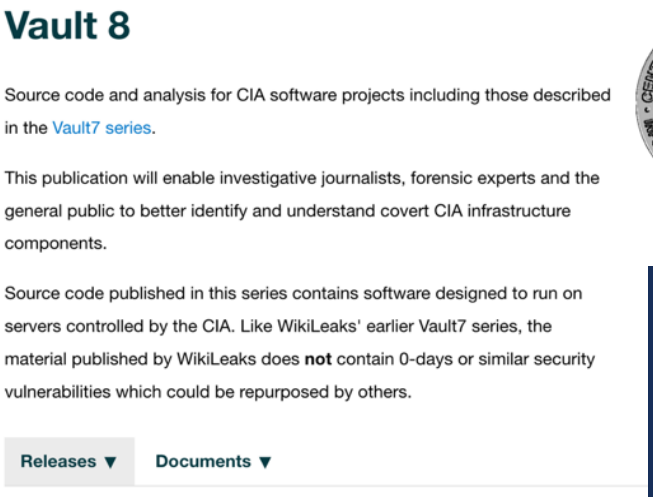

Image B - Vault 8 Screenshot

With UMBRAGE and related projects the CIA cannot only increase its total number of attack types but also misdirect attribution by leaving behind the "fingerprints" of the groups that the attack techniques were stolen from. UMBRAGE components cover keyloggers, password collection, webcam capture, data destruction, persistence, privilege escalation, stealth, anti-virus (PSP) avoidance and survey techniques."

How the release of these tools are leveling and redefining the Nation State Actor playing field

The leaked source code for these NSA and CIA cyber tools are readily available and discussed in dark web communities. Dark web enthusiasts on YouTube have posted downloadable videos walking their viewers through the specifics of these advanced exploits. While the US, China, and Russia continue to develop more sophisticated cyber weapons, other Nation-States with an emerging cyber capability can now - as a result of having access to these leaks - acquire the resources and the knowledge to attack other nation's network infrastructure and conceal the origin of the attack, further complicating the global nation station cyber environment.

The availability of such tools brings into question much of the cybersecurity's reporting around Nation-State attack attribution. For example, in early October of this year, Microsoft reported that they had witnessed 'significant' activity throughout the summer against current and former US government officials, journalists covering global politics and prominent Iranians living outside of Iran. The group Microsoft is calling "Phosophorous" made more than 2700 attempts to identify consumer accounts that could prove potential entry attack vectors. The group, believed to be from Iran, indiscriminately attacked both personal and work email addresses and attacks also included attempts at infiltrating President Trump's reelection campaign.

Recently, NSA revealed that Russian hackers from the infamous "Turla group" co-opted Iranian tools and conducted numerous attacks across industries in dozens of countries in recent months. Leveraging Iranian developed malware, Nautilus and Neuron, in combination with one of its own toolkits, called Snake, Turla obtained access to targets by scouring their networks for backdoors that had been inserted by Iranian hackers. Again, this demonstrates diffficulties in attribution.

DETECTION OF NATION-STATE ACTORS ON THE DARK WEB

As one would suspect, Nation-State Actors are not immediately apparent on the dark web. When a Nation-State launches an operational attack on an entity, or steals critical information, it has little need or desire to put that data up for sale or otherwise dump it across anonymous networks. Likewise, governments will not announce intelligence collection or law enforcement gathering activities unless for the sole purpose of psychological diversion.

After spending the last five years archiving dark web anonymous services and interacting with the dark web community, DarkOwl analysts have identified a number of Nation-State Actors "fingerprints." We see dark web these fingerprints as both indications and motivators associated with nation state actors use of anonymous networks.

Dark web Nation-State Actors have some key fingerprints that correlate to their motivating uses for the dark web.

A) Nation-State Actors use the dark web to purchase and steal cyber exploits

Nation-State Actors obtain open source cyber exploits from underground markets in order to perform reverse engineering – often to successfully construct software to counter any attack where such exploit is used against a government or critical network. A key identifier of a Nation-State Actor posing as an exploit buyer is the availability of a significant budget and financial resources to acquire the goods on offer. Regular dark web users regularly discuss 'tells' for detecting law enforcement and/or intelligence agents on the network.

B) Nation-State Actors obtain credentials on hostile governments and other entities of geo-political or military interest

For example, the dark web is replete with US *.gov email addresses that could be exploited for brute force

network intrusion or targeted phishing campaigns. As of the time of this publication, DarkOwl Vision detected over 550,000 dark web pages with credentials including a .gov email address.

Iran also has a significant government footprint of leaked credentials and network information, but it cannot be readily discerned whether this information was leaked by another Nation-State Actor or a team of vigilante hackers. For example, the hacker IranDokht is likely affiliated with a recent deep web paste by user slntar that included several dozen Government of Iran website admin panels for malicious targeting.

C) Elaborate spear-phishing campaigns are not only utilized by criminals targeting corporate networks, but Nation-State Actors employ these as well for their political and militaristic agendas

Recent reporting suggests that North Korea has successfully used phishing for obtaining access to numerous academic research organizations and critical US think tanks, using China's model for technological advancement via digital espionage. During Operation STOLEN PENCIL, North Korea targeted Stanford University's nuclear programs, proliferation, and polices group. Operation infrastructure overlapped with other campaigns conducted by North Korea. One of the IP addresses used in this campaign, (157.7.184.15) also hosted the domain bigwnet[.]com, which was used as the command-and-control infrastructure for the malware "BabyShark".

Earlier this year, DarkOwl detected an Iran-based IP address (5.160.246.99) was associated with a list of UK-government domains, specifically Her Majesty's Revenue & Customs (HMRC) in a targeted phishing campaign.

D) Nation-State Actors have used the dark web to conduct kinetic attacks against opponent's Infrastructure

In 2017, Iran conducted cyber attacks against safety systems at Saudi Arabia's Aramco, one of the largest oil producer in the world. Hackers used the Triton malware to alter one of these facility's safety controllers, which resulted in the controller shutting down an unspecified industrial process. In 2015, Russia successfully demonstrated shutting down Ukrainian power grids during political protests. Russia is also believed to be behind a number of attacks against Irish energy networks, possibly a testing ground for exploit development planned to use against more formidable opponents.

A recent release from the US CYBERCOM suggested that the US had successfully planted covert malware in Russia's electrical power grid to kinetically interrupt Russia's infrastructure in the event of a future attack, e.g. 2020 Presidential election in response to Russia accessing key nuclear safety systems in 2018.

In the summer of 2019, shortly before Black Hat 2019, Microsoft has reported in April that its Threat Intelligence Center discovered a targeted attack against IoT devices including: a voice-over-IP (VOIP) phone, a printer and a video decoder. The attack hit multiple locations, using the devices as soft access points into wider corporate networks. Two of the three devices still carried factory security settings, the software on the third hadn't been updated. Microsoft attributed the attack to a Russian group it calls Strontium, an alias for the group, Fancy Bear. Cyber security researchers have identified this group as APT28. A week ago, the same state-sponsored hacking group was linked to the hacking of the secure email accounts of researchers investigating crimes alleged to have been committed by the Russian state. Fancy Bear / APT28, Fancy Bear also key to ioT hacking (according to Microsoft).

E) Nation-States use the dark web to gain political influence by doxing political opponents

According to the Mueller report, Guccifer 2.0's successfully breached the DNC during the 2016 campaign and the information gained was carefully released to influence the US election. Numerous doxes of various key international figures on Tor's DoxBin. doxbwurbe475dm5i[.]onion. Also, President Trump has been extensively doxed with numerous examples from dark web services Cebolla and DoxBin.

F) Dark Web Propaganda

The effective use of propaganda is a key feature of a successful information operations effort. Malicious information about a political or military opponent can be leaked at critical times to influence the outcome and public opinion. The dark web contains numerous examples where government data from nations has been leaked to hidden forums and paste sites for political gain and international influence.

G) One of the most basic fingerprints of the Nation-State actors on the dark web is intelligence collection

It a widely known "secret" that key HUMINT (human intelligence) collection is conducted by Israel's Mossad and the US CIA in dark web forums, chatrooms and internet relay chats. Agents are regularly called out and teased for their overt presence in some popular dark web rooms.

Critical US defense technology has been released on the dark web and available for intelligence collection and reverse engineering by foreign adversaries. For example, last year, US military specifications for the MQ-9 Reaper Drone appeared on the dark web for sale and was widely proliferated. Sensitive information involving the MQ-9 Reaper drone and other military documents were stolen from a US Air Force captain's computer.

Open source reporting revealed that Israel's Whatsapp intelligence collection tool, Peagsus, had been deployed in 45 different countries for mobile phone collection and even sold to other countries for monitoring potential dissidents in the country in a more covert means of intelligence collection. A recent hack of Russia's contractor, SyTech discussed an effort to de-anonymize Tor, potentially revealing the true identifies of visitors to and hosts of hidden services on the dark network.

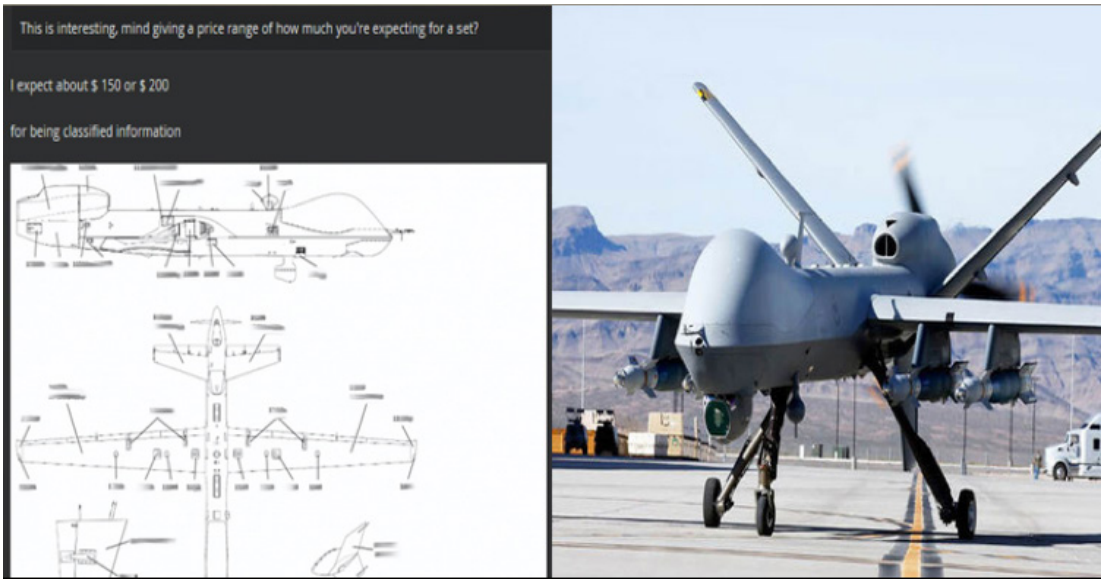

Image C- Captured from Torum

Selling US **reaper** **drone** docs
Locked

Member
Posts: 20
Joined: 21 Sep 2018
Contact:
Contact
Send private message
Selling US **reaper** **drone** docs
Report this post
Post
by » 16 Oct 2018
I am selling the US **reaper** **drone** docs for 100 dollars along with others kinds of intel. Contact me at: @protonmail.com
Top
OrangeVicar
Moderator
Posts: 193
Joined: 02 Feb 2018

Image D- Screenshot from DarkOwl Vision depicting individuals buying/selling reaper drones

NATION STATE PROXIES AND CYBER TERRORISM

Within this ever-changing threat landscape on the dark web Nation-States are also turning to proxies and levering the terrorist segment of the dark web for launching attacks and avoiding attribution. Instead of utilizing a room full of cyber-soldiers in China targeting a room full of hackers at Fort Meade (NSA) on the dark web, some Nation-States choose to leverage private "contractors" to conduct information operations on their behalf.

We believe Russia has the most extensive collection of cyber mercenaries and private contractors used by any Nation-State. In late October, open-source reports from the UK suggested the National Cyber Security Centre uncovered that the Turla Group, a cyber criminal group protected by the Russia government, had hijacked an alleged state-backed Iranian hacking group, known as OilRig or APT34, and subsequently carried out attacks on 35 countries. In July, the hacking team was actively targeting US political groups, using the code string 'TrumpTower' which coupled with the intelligence above could infer they could be linked to the alleged Iranian Phosophorous group.

Russia's contractors are also active inside Tor as well. Earlier this year, hackers, hiding under the name ov1Ru$ breached a Russian intelligence contractor, SyTech revealing a number of secretive programs targeting Tor anonymity programs. Posing as a malicious exit node in the Tor anonymous network, the contractor's program called Nautilus-S was specifically setup to deanonymize Tor traffic. The contractor, working closely with the Russian Air Force service and the FSB 71330, also had a another program in 2010 called Nautilus that harvested social media data from users of Facebook, Twitter, LinkedIn and others.

Perhaps Russia is attempting to model its behavior after the United States National Security Agency's formal relationship with its commercial contractors. For example, Booz Allen Hamiliton (BAH) has an integral alliance with the intelligence community with hundreds if not thousands of intelligence and cybersecurity specialists working alongside the NSA. Significant intelligence leaks from the NSA in recent history were facilitated by contractors such as Edward Snowden and Reality Winner, both had sensitive compartmented information access and active on behalf of the US government during their tenures with BAH. NSA and other critical intelligence community organizations will continue to solicit the support of contractors outside of the agency in order to fulfil their over national threat intelligence objectives.

Terrorists as quasi-Nation-State Actors, and the changing use of technology in the dark web

Global terrorist groups, often fueled financially and politically by certain Nation-States, have an everchanging and often reactive footprint on the dark web – reactive to the geopolitical events and policies, as well as changing technology. Many large scale extremist organizations such as ISIS, al-Qaeda, and Lebanese Hezbolla have all but declared themselves "Nation-States" in their own right, replete with military resources such as cyber armies and tactical hacking teams eager to fulfil their agendas. In the west, there is widely conflicting open source reporting as to the true activities of such quasi-Nation-States within the dark web.

A few years ago, ISIS was assessed to be extensively using anonymous networks to obscure the location and identities of its members and recruits. There were also a number of easily accessible hidden services advertising Stet-affiliated content – ISIS's Arabic language acronym – including recruitment and terrorist propaganda material. However, DarkOwl assesses with medium confidence that dark anonymous networks such as Tor will have limited future use in overt terrorist recruitment and propaganda dissemination, but instead terrorists are demonstrating a preference for encrypted mobile applications such as Whatsapp and Telegram for organizational coordination and communication.

Last year, the Wilson Center's Professor Gabriel Weinmann published an extensive report, detailing the reasons why terrorists will continue using the dark web and associated encryption communication protocols and technology. (Excerpt on following page)

[Begin excerpt]

1. "Terrorists use the dark web to hide: Extensive monitoring of the surface web by social media companies and security officials has resulted in a faster rate of removal of extremist content from social media platforms. Correlated with this is an increased use by terrorist networks of the dark web for communication, radicalization and planning attacks."

2. "Terrorists use the dark web for recruitment: While initial contact can be made on surface web platforms, further instructions are often given on end-to-end encryption applications such as Telegram on how to access jihadist affiliated websites on the dark web."

3. "Terrorists use the dark web as a reservoir of propaganda: The removal of extremist and terrorist content from the surface web increases the risk that material of terrorist organizations may be lost. Much of this content later resurfaces on the dark web."

4. "Terrorists use virtual crypto-currencies to evade detection and to fund-raise: Terrorists, like criminals, use cryptocurrency because it provides the same form of anonymity in the financial setting as encryption does for communication systems."

[End excerpt]

Image E- DarkOwl Vision Screenshot

==========

JAISH-E-MOHAMMED SOUTH INDIA

Jaish-e-Mohammed South India

Join with Us....

fight to prove our strength..

We need to strengthen our campaign in South India and america, we need more educated women from other religions to join us, we need to trap them with love, they can be moved to syria by oman corridor after conversation, our brothers bought lot of women like this from south india, below are the list of people who manage south india in social media.

We need more fund from south india, we are capable to handle the damage caused by Ayodhya verdict, we have to work on concentrating south india

Maximim Convert Hindu, Cristian Girls

https://www.facebook.com/shafeekm.sahib.1

https://www.facebook.com/salamp.hydrose

https://www.facebook.com/ranjith.l.madhavan

With respect to the argument presented in point number 2, DarkOwl continues to observe some terrorist groups, such as Jaish-e-Mohammed use the dark web to actively recruit female fighters after seeing ISIS success using jihadi brides as fighters in Iraq and Syria.

According to a dark web news outlet, at the end of 2017, researchers witnessed a surge in ISIS fundraising, specifically donations-devoted sites encouraging Bitcoin donations, confirming that ISIS cyber terrorist have awareness of the risks of financial transactions monitoring. At this time, there is no indication in DarkOwl's database that ISIS related terrorists are intentionally washing coins to evade investigative BlockChain analysis.

There are currently very limited easily discoverable ISIS or formalize terrorist group hidden services on the dark web. DarkOwl has some cataloged content from when ISIS was more active on Tor anonymous network. An example is the "Cyber Kahilafah," an effective hacking arm of the Islamic State, who in 2016 were extremely active on the dark web posting ISIS associated content such as videos and propaganda educational material. Some dark web forums suggested these were a state-run honeypot by Western governments.

Due to extensive efforts by international alliances in the "war against terrorism" there are a few terrorist groups with the infrastructure and organizational strength to coordinate widely via anonymous networks. In 2016, the international vigilante hacker group Anonymous conducted attacks against suspected members of ISIS across the dark web posting contact information for its members (email addresses social media accounts) and surface websites of its supporters, specifically Nasher Islamic State (@nashirislamicstateEN). Anonymous attacks against ISIS continued into 2019 with more Daesh/ISIS member's social media and personal information shared across multiple deep web paste services.

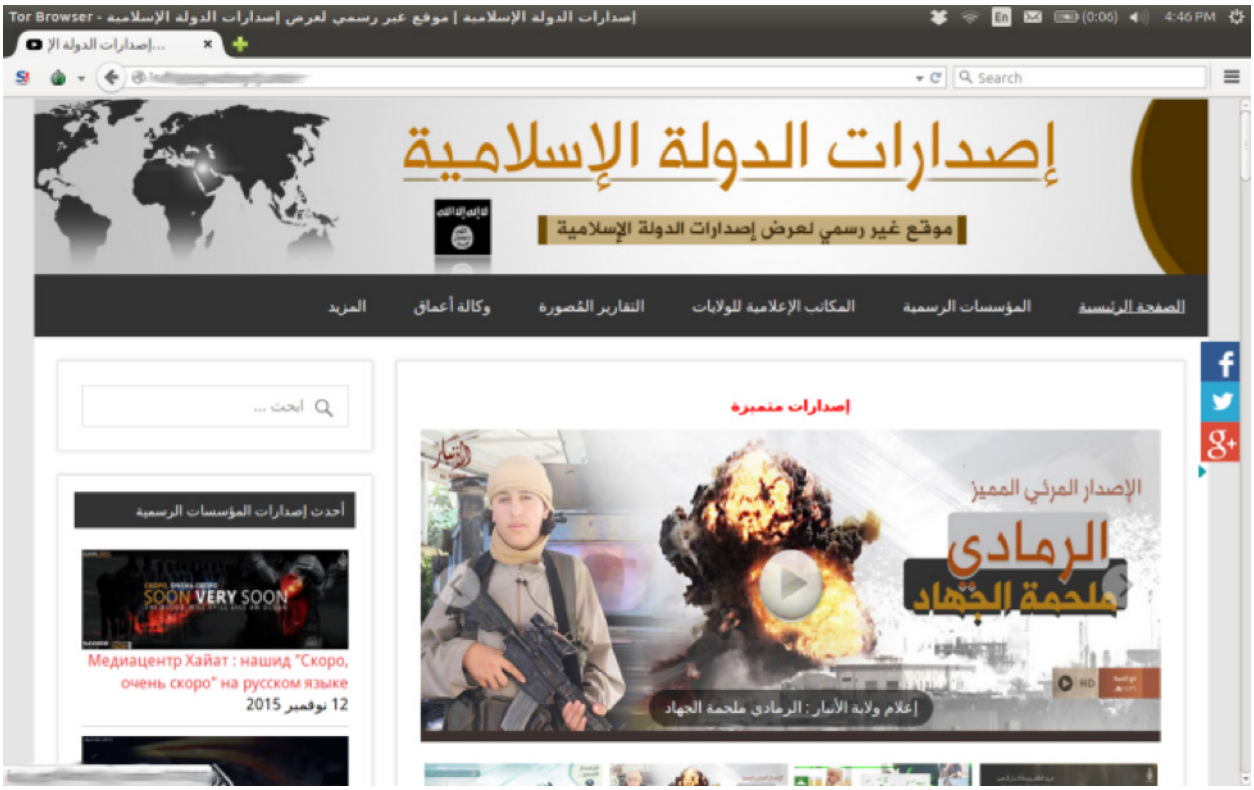

Image F- Screenshot of a former ISIS affiliated hidden Service on Tor

Such independent targeting of terrorist on the dark web continues, with content posted as recently as late September 2019 detailing the possibly geolocation coordinates of suspected ISIS leader, Abu Bakr al-Baghdadi. The dark web post closed with "ENJOY CIA" as if such information could then be used for operational targeting by the US intelligence community. Abu Bakr al-Baghdadi was killed in a US-led Special Forces operation exactly a month after the dark web posting. The coordinates pasted to the dark web did not correlate to Idlib, the location of the ISIS leader's compound and subsequent death by US security forces.

With on-going conflicts against terrorism in countries such as Syria, Iraq, Afghanistan, Yemen, and the Gaza Strip, the number of "splintered" groups is growing, especially with recent calculated attacks Turkey conducted against Kurds along the Syrian-Turkey border. There exists various imagery on Tor including videos of beheadings and executions conducted in Yemen by ISIS soldiers.

Such conflicts have caused most ISIS affiliated terrorists to shift to encrypted communication protocols such as WhatsApp and Telegram. A deep web post from July, 2019 also hinted that ISIS recruitment was even occurring in private Discord channels; Discord is a proprietary VoIP communications platform favored by the video gaming community and deep web criminals.

After Facebook acquired the popular mobile app, WhatsApp, a concerted movement to the mobile Telegram application occurred. ISIS on Telegram is growing in popularity with regular videos, pictures, links, and propaganda content despite community perception that Telegram is strict on child pornography and terrorist content posts.

A DISCUSSION WORTH CONTINUING

Nation-State and Nation-State-sponsored threat cyber actors are resourceful, employing a mix of open source and dark web assets to complete their key information operations missions. Cyber combatants, state-sponsored proxies, and teams of mercenaries utilize the dark web to conduct intelligence collection and source development, government and corporate espionage, cyber exploit development and testing, disinformation operations for geopolitical influence, infrastructure disruption, and financial gain. While unique Nation-State 'fingerprints' are identifiable in some dark web use cases, the public release of cyber weapons previously belonging exclusively to the NSA and the CIA have offered formerly less-powerful nations the ability to reframe themselves as power players, gain influence that was previously unattainable to them, and obfuscate the origin of their cyber attack, further befuddling attribution for cybersecurity researchers.

Global terrorism, frequently fueled financially and politically by specific Nation-States, have an unpredictable and often reactive footprint on the dark web – reactive to the geopolitical events and policies, as well as changing technology. Terrorists' adaptability has them shifting away from the dark web to end-to-end encrypted proprietary protocols such as Whatsapp and Telegram where they can recruit, strategize, and disseminate propaganda anonymously.

As Nation-State Actors, cyber-proxies and terrorist organizations continue to evolve in the use of the dark web and anonymizing technologies, the cybersecurity community must be vigilant to continue the conversation on intelligent identification and adaptive tracking of their everchanging tactics, techniques, and communication preferences.

Editor's note: We'd like to be clear that policing and legitimate law enforcement activity in the dark web has been intentionally compartmentalized from Nation-State Actors on the dark web in this report. We have not assumed they work independently of each other; law enforcement is a critical branch of government infrastructures and more integrally involved with smaller countries with limited resources. We have however specifically chosen not to discuss 'fingerprints' left by law enforcement on the dark web. Law enforcement have a well-known presence on the dark web hosting honey pot hidden services such as fake markets and forums, as well as posing as dark web drug vendors on popular crypto-markets to catch criminals purchasing illegal lethal drugs such as fentanyl. There are numerous open source examples where concerted international law enforcement efforts have been conducted to take down markets and pedophilia communities.

ANNEX: RANKING NATION-STATES BY CYBER INFLUENCE

Over the past several years, DarkOwl researchers have noted that Nation-States are increasingly using the dark web as an information-based battlefield for a variety of key intelligence and cyber military campaigns. In the era of digital information operations, the United States, Russia and China are the primary Nation-State actors discussed in mass media and open source reporting.

While it is true the United States, Russia and China still clearly lead in cyber-focused financial resources and manpower, there has been a significant rise of less well known Nation-States due to the release of advanced exploits leaked in recent years and available reverse engineering.

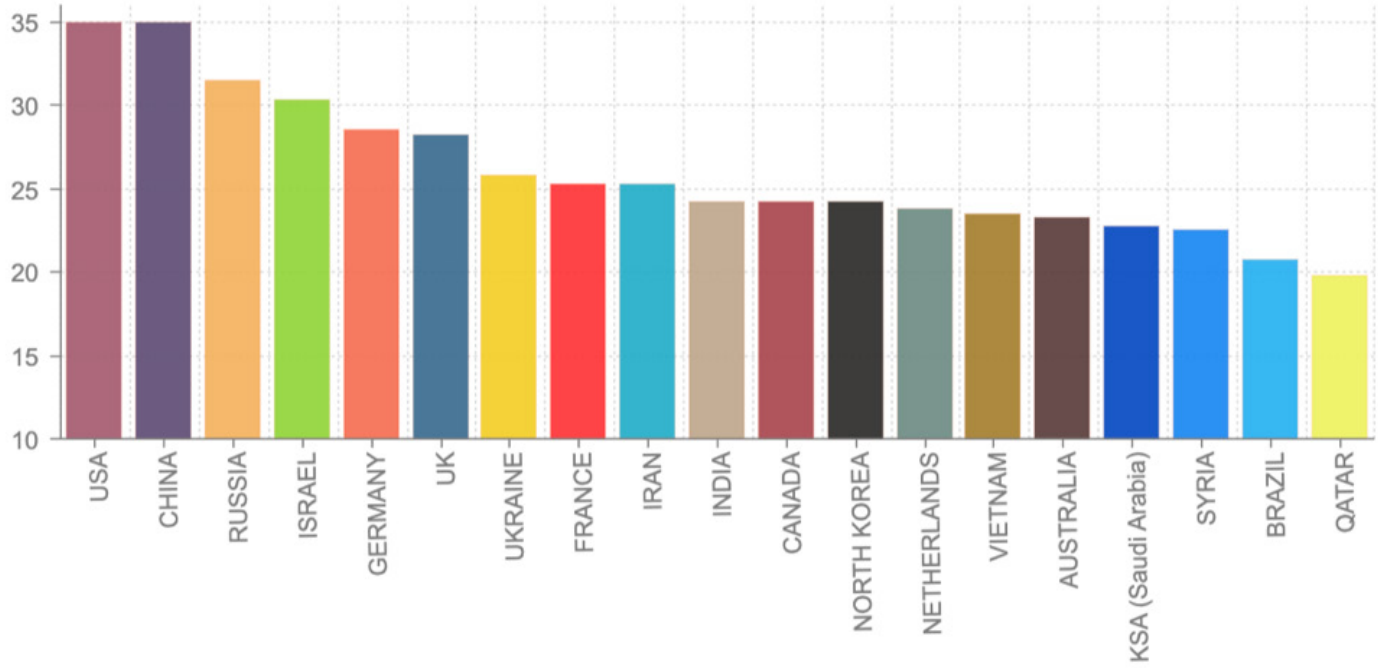

Image G - Graphic depicting the top Nation States as determined by the extent of their cyber influence

UNITED STATES

The US is plentiful in manpower, skill, finances, and international influence. The total number of cyber-soldiers employed by the US is well into the tens possibly hundreds of thousands with the recent decoupling of US Cyber Command (CYBERCOM) from the NSA and standing up its affiliated Department of Defense (DoD) branches, such as Army Cyber (ARCYBER) and Navy's FCC (Fleet Cyber Command). The US also leads in technical skill development and international influence spearheading numerous global cyber initiatives both in the dark and surface webs. In late 2019, the public learned that the US has solicited assistance from Montenegro, deploying an elite cyber team to collaborate and coordinate with in order to predict Russia's imminent influence on the US's 2020 presidential election.

CHINA

China extensively uses the deep web for espionage and intelligence collection activities. While China blocks the use of Tor to its citizens, the government regularly employs the technology's anonymity for its sophisticated PLA Unit 61398 to target US military defense technology and intellectual property. China also targets key US military defense industrial contractors for network attacks to collect designs, documents, and administrative details of critical export-controlled technology. This summer, China-based hackers were

discovered steering a large-scale cellular espionage campaign targeting 10 different mobile carriers around the world. The access realized could be leveraged to launch a future large-scale attack against cellular phone and data infrastructure. The elaborate campaign could have been orchestrated in retaliation for the on-going global 5G arms races and the US's crackdown on China's telecommunications provider, Huawei, restricting its 5G development activities in the West.

Since 2015, state-sponsored cyber PLA unit 78020 has also been involved in large-scale military, political, and economic cyber espionage in the resource-rich South China Sea area. The elaborate espionage campaign involves an intricate domain network of resources including IP addresses situated in the Denver, Colorado area according to an in-depth intelligence report published by Threat Connect, Inc.

RUSSIA

As apparent from numerous media and FBI inditements in recent years, Russia's government and intelligence services have used the surface web for numerous large scale Nation-State campaigns against targets all over the world. Attacks regularly include the US and its western allies (in what could be perceived as an all out cyber war), demonstrating a wide array of advanced technical cyber capabilities. Researchers at the Department of Defense Cyber Strategy struggle to quantify the exact number of cyber specialists available for Russian cyber campaigns, but there are reports of a number of elite dedicated operational hacking units, including 26165 and its sister unit 74455 affiliated with the hack against the Democratic National Committee and the GRU's elaborate social media campaign to influence the US election. Russia is also infamous for its use of cyber proxies, hiring advanced non-government affiliated cyber criminal organizations to conduct APT attacks on their behalf.

ISRAEL

Israel is a highly secretive and influential Nation-State Actor. Unit 8200, Israel's elite cyber spy organization is comparable to NSA with a more focused and calculated operational agenda. Unit 8200 is augmented by a number of other highly technological units with the Israeli Defense Force (IDF). Conflicting source reporting eludes to a potential dedicated Israeli Cyber Command, but those capabilities may have been distributed amongst the IDF's various telecommunications divisions at present. Former Unit 8200 personnel have also been hired by Israeli cyber corporations to implement covert activities in dark web operations that require more legal freedom and less international scrutiny.

GERMANY

Germany, the UK, and France all have sophisticated cyber capabilities. Germany has recently established its own Cyber and Information Space Command (CIR) with over 13,000 personnel assigned to ward off network intrusion attacks and disinformation campaigns. Germany law enforcement also leads in state-level dark web footprint actively participating in taking down several prominent cryptomarkets and drug vendors in recent years.

UNITED KINGDOM

Recent reporting that hackers from the United Kingdom infiltrated Russia's Turla Group highlights the sophistication of the UK's capabilities. GHCQ has doubled its capabilities from 2014, delivering full-spectrum capabilities from tactical to high end counter-state offensive cyber operations. With the UK's NHS as a principle victim to WannaCry in 2017, the UK is positioned to not only defend itself from future attacks but counter-attack when needed.

UKRAINE

Ukraine was originally not considered a prominent Nation-State Actor worth including in our analysis. In the past, Ukraine's cyber capabilities centered around organized crime and the dark web carding community. Ukraine's influence has grown, however, with Ukraine's persistent war with Russia over the annexation of Crimea, including defending against Russian cyber attack against Ukraine's electricity infrastructure. As such, we believe Ukraine to be in the top 10 Nation-State Actors in the cyber domain.

FRANCE

In early 2019, France published its new French Military Cyber Strategy consisting of two separate documents: the Ministerial Policy for Defensive Cyber Warfare (hereafter the Ministerial Policy) and the Public Elements for the Military Cyber Warfare Doctrine (hereafter the Public Elements). France has significant influence in the EU and NATO organizations making up for what it lacks in human capital for the cause.

IRAN

Iran leads in Middle Eastern countries (other than Israel) as a major Nation-State cyber actor. Iran's Cyber Army has been a formidable threat for over a decade targeting a variety of western defense and commercial networks. After the United States successfully infiltrated and shutdown their nuclear centrifuge system via the Stuxnet virus, Iran invested heavily into developing the skills and resources to hold their own on the international cyber stage. They also operate heavily in a 'proxy' configuration, where they collaborate with other smaller Nation-States to share technology and resources. It is assessed that any Nation-State-level cyber attack from Iran could be conducted with the aid of countries such as North Korea, Syria, and Yemen.

Iran has also been known to collude with terrorist organizations such as Hezbollah and private hacking groups. By training private hackers and rouge terrorists, possibly without clear direction and operational boundaries, we believe Iran could be key in orchestrating the next global cyber-war.

NORTH KOREA

North Korea has claimed responsibility for a number of large-scale attacks against international baking infrastructure in response to international economic sanctions levied against them for their resistance in ceasing their nuclear programs. According to open source intelligence reporting, North Korean hackers have successfully deployed a new ATM malware, called ATMDTrack that records and steals banking data from cards inserted in vulnerable ATMs in India. ATMDTrack is assessed to be a component of a much larger DTrack malware family that involves not only command and control remote access trojan (RAT) software, but keylogging, retrieving browser history, gathering host IP addresses, information about available networks and active connections, listing all running processes, and listing all files on all available disk volumes of the victim machine. This particular deployment points to North Korea's interest in using Nation-State cyber capabilities for money-making goals.

INDIA

In 2018, India established the National Technical Research Organisation as the main agency for protecting national critical infrastructure and to handle all the cybersecurity incidents in critical sectors of the country. Aside from cyber attacks from Pakistan, India faces attacks from other key malicious Nation-State Actors, as mentioned above with North Korea's attacks of India's banking infrastructure. Recent conflicts in Kashmir increase need for a defensive posture from vigilante hackers supporting the Kashmiri people.

CANADA

In 2018, Canada passed comprehensive legislature to empower Canada's Communications Security Establishment (CSE) for effective offensive cyber operations. The sweeping Bill C-59 positions the CSE (the Canadian NSA) to take a more "active cyber" posture as opposed to its previous defensive and reactive position. The legislation calls for the CSE to "carry out activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defense or security." Canada will not stand alone in the world stage in cyber, but have the resources and parliamentary backing to influence, protect and defend Canadian infrastructure from Nation-State attacks.

REFERENCES

Talbot, David. 2009. China Cracks Down on Tor Anonymity Network. https://www.technologyreview.com/s/415726/china-cracks-down-on-tor-anonymity-network/

DarkOwl. 2017. Shining Light On: The Electric Utilities Industry and the Darknet. https://www.darkowl.com/blog/2017/utilities-industry-and-the-darknet

Shuster, Simon and Ifraimova, Sandra. 2018. A Former Russian Troll Explains How to Spread Fake News. https://time.com/5168202/russia-troll-internet-research-agency/

Sinisterly. 2019. Hacking Exploit source code and bot exploit. Captured by DarkOwl reference: 2f98e791fda0377822b5c1a89e4e3806

Dark Rift. 2018. Hacking Topics. Captured by DarkOwl refefernce: cf4463841288febba8a7c2e871db2600

Townsend, Kevin. 2019. The United States and China - A Different Kind of Cyberwar. https://www.securityweek.com/united-states-and-china-different-kind-cyberwar

Khandelwal, Swati. 2017. Shadow Brokers Leaks Another Windows Hacking Tool Stolen from NSA's Arsenal. https://thehackernews.com/2017/09/shadowbrokers-unitedrake-hacking.html

James Munder. 2017. WIKILEAKS* CIA HACKING TOOLS Revealed VAULT 7 'Zero Day' MEGA-LEAK IS HERE https://www.youtube.com/watch?v=L7_CAoBHG-k

Matishak, Martin. 2019. Iranian hackers targeted 2020 presidential campaign, Microsoft finds. https://www.politico.com/news/2019/10/04/iran-hackers-2020-campaign-microsoft-028245

National Cyber Security Centre. 2018. Turla Group Malware. https://www.ncsc.gov.uk/news/turla-group-malware

Dream Market. 2018. Old Official Staff Thread (Page 21). Captured by DarkOwl reference: bf700aabac45074d8df5c3f11c6df3f1

Pastebin. 2019. iran admin website user: slntar-. Captured by DarkOwl reference: 8dd5a44a3934ea57e6d499816cc94fad

ASCERT Team. 2018. STOLEN PENCIL Campaign Targets Academia.https://www.netscout.com/blog/asert/stolen-pencil-campaign-targets-academia

Pastebin. 2019. HMRC-Themed Phishing Domains. Captured by DarkOwl reference: 23138c3e9de2d1566aa520b4bd415ef0

Paganini, Pierlugi. 2017. "Russian nation-state actors blamed for cyber attacks against Irish energy networks. Captured by DarkOwl reference: d163212f887bb208860af0614d4e921c

Sanger, David and Perlroth, Nicole. 2019. U.S. Escalates Online Attacks on Russia's Power Grid. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

Satter, Raphael, Donn, Jeff, and Butler, Desmond. 2017. FBI leaves US targets of Russian hackers in the dark.https://apnews.com/eb4df4898e334654a28de14dbfa7ab94

Dark Rift. 2019. Microsoft Warns Russian Hackers Can Breach Secure Networks Through Simple IoT Devices. Captured by DarkOwl reference: f1312c0d6a2218a01e050c630671d032

Cebolla. 2018. Dox Donald Trump. Captured by DarkOwl reference: 5ca5a9a1449319ede746c490dbd90eb5

DoxBin. 2016. Donald Trump DoX. Captured by DarkOwl reference: be712b81fa1d5e47b4d935cc6556dfd4

The New Arab. 2019. Guardian 'targeted by Saudi hacking unit' after Khashoggi murder. https://www.alaraby.co.uk/english/news/2019/6/19/guardian-targeted-by-saudi-hacking-unit-after-khashoggi-murder

8chan Tor Service. 2018. Dude did you hear? The CIA is here. Captured by DarkOwl reference: 90b9558df41a71c66df43aad7db6d378

Torum. 2018. Selling US reaper drone docs. Captured by DarkOwl reference: 0e23f004fabe07a02b6074e70f6ff58f

Cimpanu, Catalin. 2018. 'Lawful intercept' Pegasus spyware found deployed in 45 countries. https://www.zdnet.com/article/lawful-intercept-pegasus-spyware-found-deployed-in-45-countries/

Robinson, Teri. 2019. Russian Turla group masqueraded as Iranian hackers in attacks. https://www.scmagazine.com/home/security-news/apts-cyberespionage/russian-turla-group-masqueraded-as-iranian-hackers/

Echo of Russia. 2019. The most serious FSB leak ever (Самая серьезная утечка, когда-либо случавшаяся в ФСБ). https://ehorussia.com/new/node/18934

Shorrock, Tim. 2015. How Private Contractors Have Created a Shadow NSA. https://www.thenation.com/article/how-private-contractors-have-created-shadow-nsa/

Weimann, Gabriel. 2018. Going Darker? The Challenge of Dark Net Terrorism. https://www.wilsoncenter.org/sites/default/files/going_darker_challenge_of_dark_net_terrorism.pdf

Pastebin. 2019. Jaish-e-Mohammed South India. Captured by DarkOwl reference: 697a16d9e68040c5ca52f460a6d9ae77

Dark Web. 2018. Analysis: The Rise of Bitcoin and Cyber-Terrorists. Captured by DarkOwl reference: 583d81dda4bc72c137799bb020004582

انجازات – CyberCK. 2016. Captured by DarkOwl reference: de1c63aecc69e4331f4623648b915411

Former ISIS Affiliated Hidden Service on Tor 2016. http://isdratetp4donyfy[.]onion

Pastebin. 2016. 8-May-2016. Captured by DarkOwl reference: f65a8690ebbde088c9ccdfc7c85305d2

Pastebin. 2019. 2019-04-25T05:26:56.000Z, List of terrorist sites. Captured by DarkOwl reference: 85b33f94eeed0e3148ec91b577a0a306

AlJazeeera. 2019. ISIL chief Abu Bakr al-Baghdadi killed in Syria, confirms Trump. https://www.aljazeera.com/news/2019/10/isil-chief-abu-bakr-al-baghdadi-killed-syria-confirms-trump-191027132540524.html

DeepPaste. 2019. Abu bakker Al-baghdadi Location. Captured by DarkOwl reference: 79f158a01f3b6058d4923dd85f74d92b

CBS News. 2019. ISIS releases new footage of leader Abu al-Baghdadi for first time in 5 years. https://www.cbsnews.com/news/al-baghdadi-isis-releases-new-footage-of-leader-abu-bakr-al-baghdadi-today-2019-04-29/

Heras, Nicholas. 2016. Fighting Terrorism in Syria: It's More Than ISIS. https://nationalinterest.org/feature/fighting-terrorism-syria-its-more-isis-16294

The Hacker Bays. 2019. Islamic State Execution by Tank. Captured by DarkOwl reference: 5506df25082235b8e0d59bd9ba92413b

Pastebin. 2019. Untitled: ISIS Recruitment. Captured by DarkOwl reference: bbbe0757e4b79b72e65820411b920473

Telegram. 2019. Channel: اصدارات طباور. Captured by DarkOwl reference: e6592785b22bec5a34f950dbf52cba

Telegram. 2019. Supergroup: Blank World. Captured by DarkOwl reference: f450212cf7f4e09934f04f88d8aedc6c