Dancho Danchev's Offensive Cyber Warfare Articles Compilation for Unit-123.org

BY DANCHO DANCHEV

The Top 10 Off-The-Shelf Cyber Threat Intelligence Career Positions – And Which One You Should Pick Up? – Cyber Intelligence Products – Mobile E-Shop

Every then and now a logical question emerges – which are some of the most relevant cyber threat intelligence positions and which one you should aim at excelling at in terms of applying as soon as possible and what are some of the necessary skills and qualifications required for you to join the vibrant world of defensive and offensive cyber warfare? Keep reading.

In this post I'll walk you through ten currently active and possibly high-profile hot cyber threat intelligence careers that you could possibly get involved in in terms of applying including to actually offer pragmatic and market-segment relevant advice on how to master them and excel at these careers.

Among the key cyber threat intelligence career positions that are on the top and off-the-shelf from major defensive and offensive cyber warfare vendor providers currently include:

Threat Hunter – this is one of the new and currently highly demanded position that's beginning to take shape across the threat intelligence market segment which basically has to do with active Big Data using public and proprietary sources data mining for malicious software and malicious campaigns. Among the key prerequisites for this position is basic OSINT understanding and experience including knowledge of various TTPs (tactics techniques and procedures) in terms of how exactly is today's modern malware making its way on a corporate network including personal and home PCs in particular generic possibly in-depth knowledge of various currently in-the-wild botnets and malware families including various other ways in which today's modern malicious and fraudulent campaigns are making their way on corporate networks including home and personal PCs. Possible sources of current and historical information on IoCs

(Indicators of Compromise) and TTPs (tactics techniques and procedures) which you can catch up include my personal **blog** . Among the first services which you should begin to utilize in terms of crowd-sourced public community driven OSINT type of information and data repositories include – **VirusTotal** , **Hybrid-Analysis** , **ANY.RUN** , **AMAaaS** , **Intezer Analyze** , **IRIS-H Digital Forensics** , **CAPE** , **Valkyrie** , **JoeSandbox** which should offer a pretty decent set of malicious activity for you to play with in terms of enriching your personal knowledge and experience in the field of Threat Hunting.

SIGING Assets Discovery – this is a relatively high-profile position within the military and the defense sector including the U.S Intelligence Community in the context of empowering the employer with the necessary data information and knowledge in terms of keeping track of and discovering new and relevant new and currently circulating in-the-wild cyber threats including possible targets-of-opportunity with the actual data potentially utilized for offensive Tailored Access Operations including possibly to establish "touch points" with a targeted infrastructure for the purpose of launching both passive and active defensive and offensive cyber warfare campaigns. Among the key requirements for this position is a solid OSINT experience and know-how including automated use of popular Data Mining and Social Network Analysis tools for the purpose of building active network and actual individual dossiers including the active execution of defensive and offensive cyber warfare operations against network-based infrastructure including possibly an individual or a set of individuals in question. The key point here is to actually have the strong analytical and OSINT-based analysis tools to proactively spot and detect current and ongoing major or targeted phishing and spam including malicious-software distributing campaigns for the purpose of properly profiling the activity of the gang including to actually be able to properly perform a passive or active network reconnaissance of a targeted infrastructure for the purpose of establishing the foundations for a successful Tailored Access Operation against a particular target or a set of targets.

Offensive Cyber Warfare Operator – this position requires basic understanding of Network fundamentals including active OSINT experience and actual passive and active network and infrastructure-based reconnaissance experience for the purpose of launching and actually orchestrating defensive and offensive cyber warfare operations against the network or the actual individual. The main purpose behind this career position would be to actually orchestrate and operate a defensive and offensive Cyber Warfare platform including possible to launch and orchestrate virtual SIGINT missions including possibly Tailored Access Operations using a pre-defined set of proprietary and of-the-shelf offensive cyber warfare tools.

OSINT Analyst – This is among the most popular and currently sought after position in the field of Cyber Threat Intelligence where experienced masters of OSINT (Open Source Intelligence) can easily make a career by beginning and actually starting to profile malicious and fraudulent actors by using Open Source Intelligence tools and methodologies. Among the key success factors for this position is the actual use of public and proprietary OSINT tools and techniques including personal and publicly discussed and proposed methodologies.

Tailored Access Specialist – Do you like doing unethical penetration testing? Do you easily go for signing an NDA? This is yet another currently hot position on the Cyber Threat Intelligence front where you can easily aim to and attempt to compromise a malicious adversary's network potentially compromising it and actually exposing the true face of a malicious and fraudulent campaign including to actually assess the damage and include a victim's list.

Virtual HUMINT Analyst – Do you have a lot of experience hanging around cybercrime forum communities? Are you good at spotting valuable cybercrime-friendly underground market propositions and actually initiating a conversation with the actual owner of the service for the purpose of gathering intelligence on the service including the true scope of the fraudulent proposition? Keep reading. This is among the key Cyber Threat Intelligence market-segment positions where the actual analyst would further profile and attempt to infiltrate a specific cybercrime-friendly service including to infiltrate a specific cybercrime forum community for the purpose of "processing" it using automated OSINT gathering tools including possible use of personal methodologies. The key success factors here are often the use and reliance on basic Intelligence Gathering principles including the use of social engineering. Brace yourselves – and make sure that you have a decent budget on your behalf in the very beginning.

Cyber Technical Collector – Have you ever dreamed of processing and obtaining full access to a cybercrime forum community for the purpose of taking a deeper look inside its market-segment leading fraudulent and rogue propositions? The main purpose behind this position is to actually be in a position to gather as much information about a specific cybercrime forum community including to build a list of cybercrime-friendly communities for the purpose of automatically processing them using automated OSINT tools and possible use of personal OSINT methodologies and public and proprietary tools.

Big Data Cyber Visualization Expert – The main purpose behind this position is to establish the foundation for a successful visualization of cybercrime-friendly forum community data possibly generating graphs and charts including actual visualization of a Social Network Analysis of all the participants within a specific fraudulent and rogue cybercrime-friendly forum community.

Cybercrime Researcher and Expert – This is among the hottest positions within the Cyber Threat Intelligence market-segment where the actual research and expert would have to posses a decent understanding of various trends within the cybercrime ecosystem including how it works and how cybercriminals actually monetize the fraudulent campaigns using alternative payment methods and possible cash-out strategies including to actually be in a position to prevent and offer practical and technical recommendations for the mitigation of this type of activity.

Cyber Threat Intelligence Analyst Linguist – Do you know several languages? Are you experienced in fighting cybercrime? Are you technically sophisticated enough to fight malware? This is an ideal position for you to take advantage of in terms of localizing cybercrime forum community content and actual fraudulent propositions to another language possibly breaking the language-barrier and actually empowering your employer with the necessary information on stay on the top of their game.

Are you interested in finding out more about currently active and hot Cyber Threat Intelligence Careers and possibly get hands-on experience and training in Information Warfare OSINT and Cyber Warfare?

Approach me at [email protected]

dancho.danchev

See author's posts

Tags: Cyber Actor Attribution , Cyber Arsenal , Cyber Arsenal Build-Up , Cyber Assets , Cyber Assets Inventory , Cyber Attack Attribution , Cyber Espionage , Cyber Threat Attribution , Cyber Warfare , Cyber Warfare Doctrine , Defensive Cyber Warfare , Offensive Cyber Warfare , United States Cyber Warfare Doctrine

Continue Reading

Previous Exploring the Basics of Cyber Assets and Cyber Inventory Efforts Build-up – A Proposed Off-the-Shelf Methodology

Exploring the “Let’s Name and Shame Them” Intelligence Community Mentality – Keep it coming? – Cyber Intelligence Products – Mobile E-Shop

Is it just me or I think that what was once basically classified and sensitive information is becoming to make its way into the public space including the commercial sector for the purpose of disinforming or generating revenue for its owners including with the actual information and research making it in places where you could once dream of seeing it – such as for instance **FBI’s Most Wanted Cybercriminals** list? Keep reading.

When was the last time you really knew what APT (advanced persistent thereat) really means? Do you think it’s suitable even common for the FBI to actually feature major and prominent cyber espionage groups into its most wanted Cybercriminals list largely utilizing and using public sources or eventually based on complaints? Think twice before featuring these groups – or else everyone can make it in the FBI’s Most Wanted Cybercriminals list based on the research that they do which could possibly lead to a direct compromise of OPSEC (Operational Security) despite the given and offered rewards.

Let’s take a brief look at the **FBI’s Most Wanted Cybercriminals list for 2020** and discuss in-depth the general mentality of “naming and shaming” bad actors including the rare cases where bad actors try to “name and shame” the good actors and discuss in-depth the intersection between law enforcement and the U.S Intelligence Community and the Security Industry in terms of obtaining and actually acting upon classified and potentially sensitive cyber threat intelligence in an attempt to raise more awareness on the actual usability and potential irrelevance and possible mockery of utilizing Security Industry driven cyber threat intelligence which basically comprises a decent port of the individuals and groups currently found on the FBI’s Most Wanted Cybercriminals Top List.

Find below related information on some of the key individuals currently on the FBI's Most Wanted Cybercriminals Top List:

Innovative Marketing Evgeniy Mikhaylovich Bogachev Syrian Electronic Army Iranian-Based Cyber Threat Actors

The threasure-throve of cyber threat intelligence information currently at the disposal of the U.S Intelligence Community can be also greatly attributed to the ongoing commercialization of the threat intelligence market segment with more vendors and feed providers actually joining this market segment potentially offering thousands of never-published before IoCs (Indicators of Compromise) and in-depth discussion and actual data-mining for advanced persistent threats which can be greatly described as passive vitual SIGINT and actual tactics techniques and procedures (TTPs) discussion which I've been basically doing for over a decade now.

How should the U.S Intelligence Community actually respond to the ongoing mockery and complete IP (Intellectual Property) theft in terms of the ongoing commercialization of the threat intelligence market segment? As I've once discussed before and actually participated in a Top Secret GCHQ Progam aiming to monitor public hacker and security expert Twitter feeds for OSINT (Open Source Intelligence) data called "**Lovely Horse** " the overall reliance on the commercial sector in combination with the academic sector could truly prove to be a valuable and extremely positive in terms of a potential central clearing-house of cyber threat intelligence events which could greatly mature into a commercial-academic and U.S Government private sector partnership with the U.S Intelligence Community potentially diversifying the technical know-how and potential sources of information citing possible National Security considerations in place.

It should be fairly easy to assume that the day advanced persistent threats (APTs) start popping-up on the FBI's Most Wanted Cybercriminals Top List with tons of publicly obtainable or commercially available information and data on a given case we can easily begin to talk and discuss the actual OPSEC (Operational Security) compromise of the actual campaign to track down and prosecute the individuals behind a specific campaign.

With more vendors continuing to generate buzz including possibly sales on a per advanced-persistent-threat (APT) basis it should be fairly easy to assume that good old fashioned free and publicly accessible and obtainable sources of strategic tactical and operational cyber threat intelligence should continue to represent your daily read and daily visit.

dancho.danchev

See author's posts

Tags: Advanced Persistent Threat , APT , Cyber Actor Attribution , Cyber Attack Attribution , Cyber Threat Attribution , FBI , FBI Most Wanted , FBI Most Wanted Cyber , FBI Most Wanted Cybercriminals , Intelligence , Intelligence Community , Operational Security , OPSEC , Tactics Techniques and Procedures , TTP

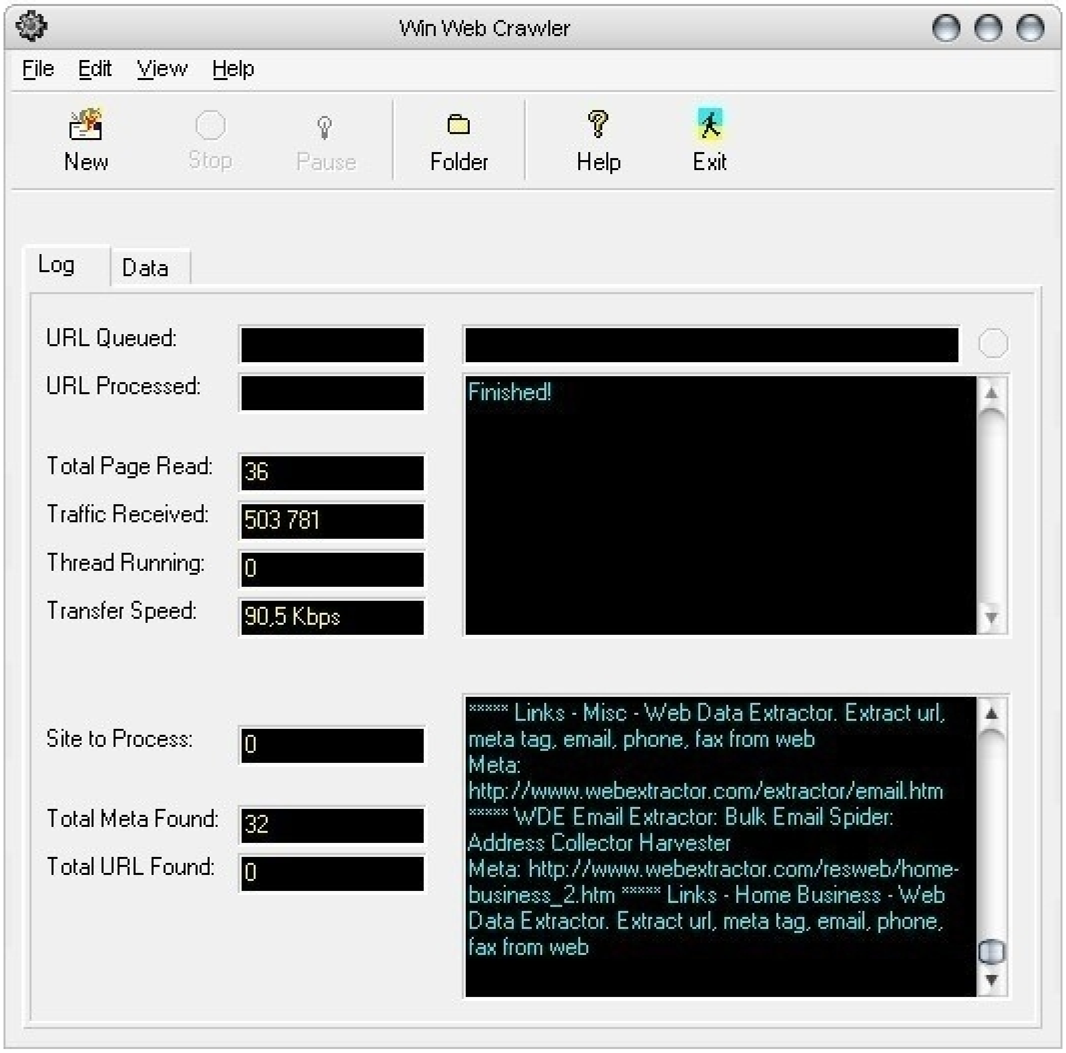
Exploring the Basics of Cyber Assets and Cyber Inventory Efforts Build-up – A Proposed Off-the-Shelf Methodology – Cyber Intelligence Products – Mobile E-Shop

It should be clearly noted that every decent Cyber Warrior including potential wannabe Cyber Warriors should clearly possess the necessary data information and knowledge including Offensive and Defensive Cyber Warfare experience and tradecraft for the purpose of establishing the foundations for a successful cyber operational Cyber Assets and Cyber Inventory efforts build-up.

In this post we'll walk you through a proposed off-the-self Cyber Assets and Cyber Inventory Assets build-up methodology with the idea to provide Unit-123 users with the necessary "know-how" and information to successfully implement manage and operate Cyber Assets and Cyber Inventory efforts build-up cyber operational defensive and offensive Cyber Warfare Program. Keep reading!

Among the primary key summary points that we'll highlight in this analysis include:

Cyber Assets Inventory Build-Up – What does a Cyber Asset constitute? Basically it's a virtual or in some cases physical cyber security or a hacking item that can be further utilized or eventually weaponized for the purpose of achieving a cyber operational capability further empowering the Cyber Warrior with the necessary tools-of-inventory on their way to achieve their cyber operational objective. What would be a suitable example for a virtual or physical Cyber Asset? Keep reading. Among the key virtual and physical assets that we'll highlight in this post for the purpose of building an Information Warfare Workstation including Information Warfare-based type of terminal include – Multiple online accounts, years long online identity and cyber persona reputation, general understanding of the cyber threat landscape, online backup of crucial online data, offline backup of crucial online data, historical OSINT type of data repository online and offline backup type of data, established online Web properties including loyal user base including loyal online traffic base. Let's offer a detailed overview of some of the highlighted offline and online assets for the purpose of elaborating more on the basics behind establishing the foundations for a successful Cyber Warrior type of training career. Among the key points that every Cyber Warrior including wannabe Cyber Warriors should consider is to obtain access to multiple online accounts including possibly LinkedIn Twitter and Facebook further positioning his or her experience in the field including current understanding of Offensive and Defensive Cyber Warfare including but not limited to an IM (Instant Messaging) account such as for instance Skype or XMPP type of account where you can socialize and network with colleagues including fellow researchers and Cyber Warriors including possibly wannabe Cyber Warriors.

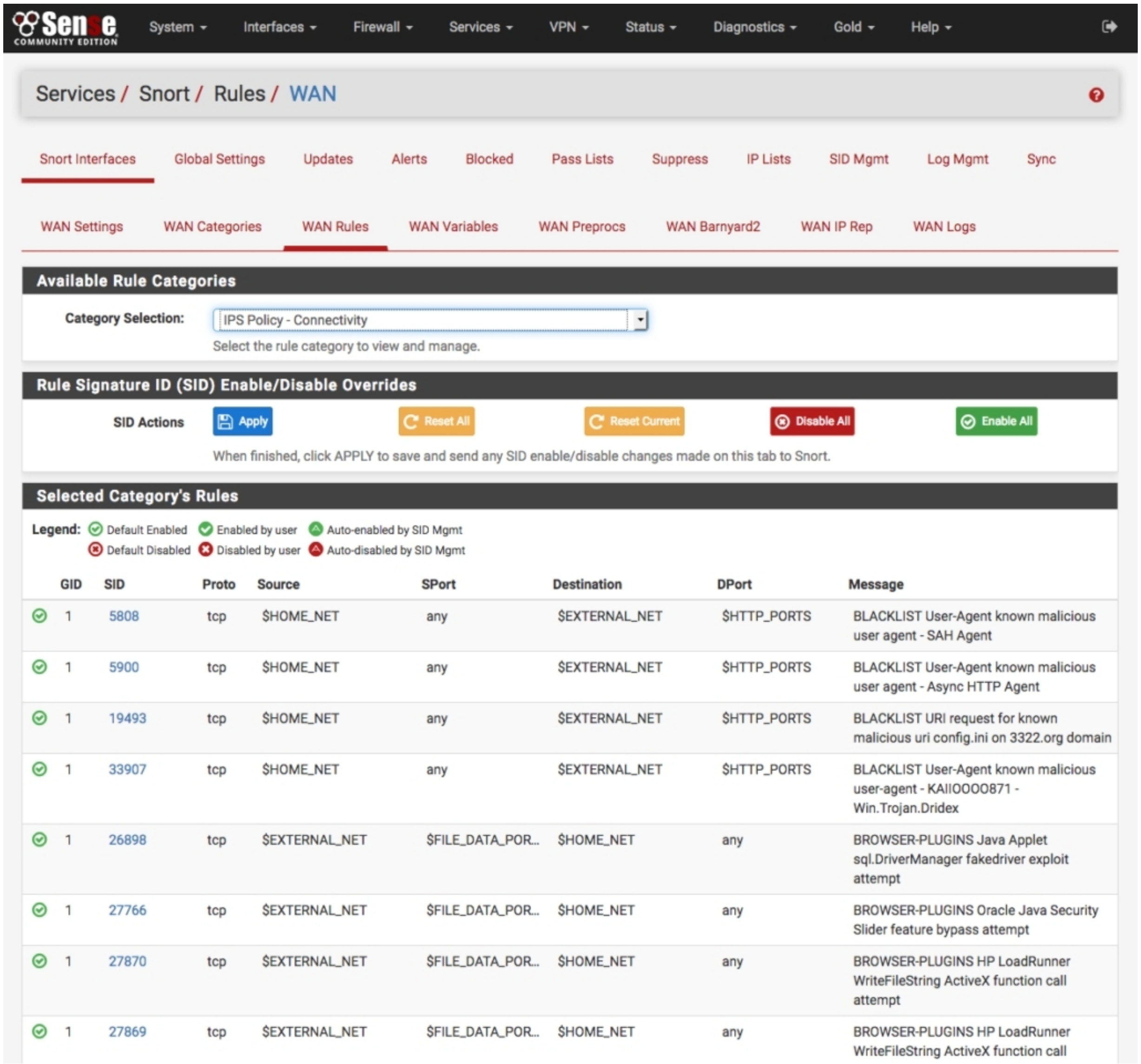


```
URL Queued:
URL Processed:

Total Page Read:     36
Traffic Received:    503 781
Thread Running:      0
Transfer Speed:      90,5 Kbps

Site to Process:     0

Total Meta Found:    32
Total URL Found:     0
```

```
Finished!
```

```
***** Links - Misc - Web Data Extractor. Extract url,
meta tag, email, phone, fax from web
Meta:
http://www.webextractor.com/extractor/email.htm
***** WDE Email Extractor: Bulk Email Spider:
Address Collector Harvester
Meta: http://www.webextractor.com/resweb/home-
business_2.htm ***** Links - Home Business - Web
Data Extractor. Extract url, meta tag, email, phone,
fax from web
```

Cyber Arsenal Inventory Build-Up – Among the key concepts behind the establishment of a possible Cyber Arsenal Online and Offline Inventory Build-up include access to a commercial and off-the-self Virtual Private Network (VPN) access, access to an encrypted email including active use of Pretty Good Privacy (PGP), access to online Web Crawler for the purpose of performing online sentiment and online trends analysis, multiple and well-established personal network of personal contacts including U.S Intelligence Community personnel, including academic and Security Industry contacts including possible old-school popular and well-known hacker and Security Researchers type of contacts.



Services / Snort / Rules / WAN

Available Rule Categories

Category Selection: IPS Policy - Connectivity

Select the rule category to view and manage.

Rule Signature ID (SID) Enable/Disable Overrides

SID Actions

When finished, click APPLY to save and send any SID enable/disable changes made on this tab to Snort.

Selected Category's Rules

Legend: ✓ Default Enabled ✓ Enabled by user ▲ Auto-enabled by SID Mgmt
⊗ Default Disabled ⊗ Disabled by user ▲ Auto-disabled by SID Mgmt

	GID	SID	Proto	Source	SPort	Destination	DPort	Message
✓	1	5808	tcp	$HOME_NET	any	$EXTERNAL_NET	$HTTP_PORTS	BLACKLIST User-Agent known malicious user agent - SAH Agent
✓	1	5900	tcp	$HOME_NET	any	$EXTERNAL_NET	$HTTP_PORTS	BLACKLIST User-Agent known malicious user agent - Async HTTP Agent
✓	1	19493	tcp	$HOME_NET	any	$EXTERNAL_NET	$HTTP_PORTS	BLACKLIST URI request for known malicious uri config.ini on 3322.org domain
✓	1	33907	tcp	$HOME_NET	any	$EXTERNAL_NET	$HTTP_PORTS	BLACKLIST User-Agent known malicious user-agent - KAII0000871 - Win.Trojan.Dridex
✓	1	26898	tcp	$EXTERNAL_NET	$FILE_DATA_POR...	$HOME_NET	any	BROWSER-PLUGINS Java Applet sql.DriverManager fakedriver exploit attempt
✓	1	27766	tcp	$EXTERNAL_NET	$FILE_DATA_POR...	$HOME_NET	any	BROWSER-PLUGINS Oracle Java Security Slider feature bypass attempt
✓	1	27870	tcp	$EXTERNAL_NET	$FILE_DATA_POR...	$HOME_NET	any	BROWSER-PLUGINS HP LoadRunner WriteFileString ActiveX function call attempt
✓	1	27869	tcp	$EXTERNAL_NET	$FILE_DATA_POR...	$HOME_NET	any	BROWSER-PLUGINS HP LoadRunner WriteFileString ActiveX function call

Practical Network-Based Infrastructure and Host-Based OPSEC Advice – Among the key concepts to consider is basic host-auditing using both software and hard-ware based isolation concepts including the presence and existence of "malware-free" type of online host for the purpose of doing cybercrime and Threat Intelligence including Information Security type of research including an active access to a proprietary VPN (Virtual Private Network) service including a decent and daily maintenance of basic situational awareness in terms of new cyber threats and cybercrime including basic geopolitics knowledge and understanding.

The ultimate goal? To dominate the Cyber Threat Landscape with data information and knowledge and to further reach out to a new generation of Cyber Warriors potentially launching or joining a Community-of-Interest and contributing to a bigger cause – The U.S Intelligence Community and the general U.S Government including the DoD's understanding of offensive and defensive cyber warfare practices and doctrines.

Recommended Tools and Online Services:

RSS Reader – http://www.rssowl.org
Proprietary VPN Service Network – https://www.cryptohippie.com
Network-Based Deception – https://deepbluesecurity.nl
Hardware Isolation – https://www.pfsense.org
Web Crawler – https://www.httrack.com
OSINT Enrichment – http://project.carrot2.org
Host-Based Search Engine – https://yacy.net
Zero-Knowledge Backup – https://spideroak.com

dancho.danchev

See author's posts

Tags: Cyber Arsenal , Cyber Arsenal Build-Up , Cyber Assets , Cyber Assets Inventory , Cyber Warfare , Cyber Warfare Doctrine , Defensive Cyber Warfare , Information Warfare , Offensive Cyber Warfare , Operational Security , OSINT , Security , United States , United States Cyber Warfare Doctrine

Continue Reading

Previous DoD's Cyber Strategy – 2018 – Shall We Play a Cyber-Retaliation Game? Next The Top 10 Off-The-Shelf Cyber Threat Intelligence Career Positions – And Which One You Should Pick Up?

DoD’s Cyber Strategy – 2018 – Shall We Play a Cyber-Retaliation Game? – Cyber Intelligence Products – Mobile E-Shop

Building offensive cyber warfare and intelligence-gathering capabilities? Further positioning China and Russia as pre-dominant Cyber Warfare powers? Departamentalization and ongoing consolidation of different Offensive Warfare cyber groups? Keep reading.

We’ve recently obtained access to the currently accessible DoD Cyber Strategy for 2018 – and decided to further take a deeper look potentially communicating invaluable information and related data to Unit-123.org readers further highlighting and elaborating more on some of the key points of DoD’s Cyber Strategy for 2018.

Key points include:

Real-time based ongoing offensive Cyber Warfare build-up and Cyber Threat Intelligence gathering operations – Want to be a Journeyman? Want to keep track of the latest cyber threats to the bottom of the source potentially undermining a malicious and fraudulent campaign? Keep reading. The U.S DoD is currently busy establishing the foundations for what can be best described as day-to-day Offensive Cyber Warfare operations and Intelligence-gathering operations in the context of what I managed to archive circa 2008-2012 when I managed to successfully keeping track and eventually launching a take down effort against the Koobface botnet following two and a half years daily and active campaign monitoring and take down efforts – while undertaking the position of Journeyman on my way to successfully keep track of and undermine various Koobface related malicious and offensive Cyber Warfare activities. What’s worth pointing out is that day-day-operations can potentially lead to a lower level of OPSEC (Operational Security) in terms of properly attributing a variety of nation-state and malicious and fraudulent groups based cyber attacks. What readers including the U.S DoD should keep in mind is that a properly trained Cyber

Warrior can truly make impact in terms of becoming a Journeyman in case a proper OPSEC (Operational Security) practice and experience is in place including a possible experience with long-term and short term Cyber Assets build-up can really take place. Don't have the necessary experience in building-up a Cyber Assets arsenal and information repositories? Think twice before engaging in day-to-day Cyber Warfare operator positions in terms of having the necessary experience in building up Cyber Assets and cyber arsenal type of information and account repositories. How should a potential Cyber Warrior proceed in terms of building-up a proper Cyber Assets repository including a possible Cyber Warfare arsenal? Keep reading. It should be noted that properly built and stashed Cyber Assets including Cyber Warfare arsenal is crucial for maintaining day-to-day offensive Cyber Warfare operations including possible Intelligence-gathering operations. Stay tuned for an upcoming in-depth analysis of the basic principles of Cyber Assets and offensive Cyber Warfare arsenal build-up basics.

Further enhancing cyber threat intelligence collection capabilities – The next point in the most recently obtained DoD Cyber Strategy for 2018 has to do with enhancing and improving Intelligence collection and gathering operations. Welcome to the Wonderful World of industry-automated OSINT? Or shall we play a cyber retaliation game? Keep reading. The current state of OSINT has to do with a variety of independent-based consultants and Intelligence Analysts spreading data information and knowledge successfully enriching and enhancing public data sets and data-mining social media for active personal threat actor profiling largely provoked by the **infamous quote** by U.S President Nixon courtesy of the CIA – "*What use are they? They've got over 40,000 people over there reading newspapers.* ". Largely relying on a variety of proprietary and publicly obtainable OSINT-based type of automated tools including a proprietary and custom-based OSINT trade-craft and methodology – the current state of the OSINT industry seems to be in a favorable stance courtesy of the U.S Intelligence Community successfully fueling growth into a variety of different market segments potentially empowering the U.S Intelligence Community with the necessary data information and knowledge to stay on the top of its game. An OSINT conducted today is a tax payer’s dollar saved tomorrow.

Striking back where it hurts most – at the source – In a world dominated by popular buzz-words including “stepping-stones” and Iran-based “proxies” including Russian and China’s utilization of civilian sector for the purpose of launching orchestrating and managing offensive cyber warfare campaigns – it shouldn’t be surprising that striking back at the source remains among the primary and top priorities of the U.S Intelligence Community. In a world dominated by public and proprietary-obtainable OSINT sources – it shouldn’t be surprising that the U.S Intelligence Community including its partners are perfectly positioned to obtain the necessary data information and knowledge to stay on the top of its game. Intersecting CYBERINT with virtual HUMINT for the purpose of reaching to law enforcement agencies including the U.S Intelligence Community and the general public should be considered as a proactive option in terms of reaching out to and prosecuting high-profile and low-profile cybercriminals including the active profiling of various cybercrime-friendly communities for the purpose of establishing the footprint of an active forum and community-infiltration tactics. Yet another scenario worth profiling is the active utilization of government-sponsored and orchestrated DDoS (Denial of Service Attacks) utilizing commercial and government-owned and positioned infrastructure for the purpose of denying an enemy the option to properly utilize their online assets potentially undermining his and their cybercrime-friendly community’s ability to remain online potentially undermining public confidence in the cybercrime-friendly community leading to a potentially disrupted online rogue and fraudulent operation.

Waging full-spectrum offensive Cyber Warfare capabilities build-up – What does full-spectrum cyber warfare really mean? It basically means spending a decent amount of money to properly outsource the necessary “know-how” including technical solutions in terms of defensive and offensive cyber warfare to a variety of leasing military complex contractors. Among the key recommended summary points in this particular case would be to properly build a law enforcement and private sector community outreach for the purpose of establishing the foundations for active data-and-information sharing including the necessary dissemination of active threat intelligence further enhancing the U.S Intelligence Community's capabilities in terms of properly responding to and proactively preventing major including targeted cyber attacks. Establishing the foundations for a successful data-and-information sharing repository consisting of threat intelligence data including data-and-information on current and emerging major and targeted cyber attacks should be considered as an option for the purpose of establishing the foundations for a successful threat intelligence data type of repository.

Long-term and short-term Security Industry and commercial sector build-up – Among the most common myths in terms of ongoing cooperation with law enforcement and the private sector including the academic market segment would be the direct establishment of a central data-and-information repository including the exchange of threat intelligence data and OSINT know-how. What should be clearly done in this particular area would be to establish an active community and industry outreach program whose purpose would be to properly recruit train and educate including the active exchange of threat intelligence data including academic insight into the area of threat intelligence gathering cybercrime research and malicious software research and analysis projects including newly launched commercial and private ventures including R&D projects in the area of cyber security.

dancho.danchev

See author's posts

Tags: Cyber Warfare , Department of Defense , DoD , DoD Cyber Strategy , DoD Cyber Strategy 2018 , Information Warfare ,

Offensive Cyber Warfare , Security , United States , United States Cyber Warfare Doctrine

Continue Reading

Previous Proactively Digging in the U.S Cyber Warfare Realm – And How You Can Perform Better? Next Exploring the Basics of Cyber Assets and Cyber Inventory Efforts Build-up – A Proposed Off-the-Shelf Methodology

Proactively Digging in the U.S Cyber Warfare Realm – And How You Can Perform Better? – Cyber Intelligence Products – Mobile E-Shop

Do you want to become a major Cyber Warfare player? Do you want to effectively assist your Unit organization or nation in becoming a major Cyber Warfare power? Keep reading.

In this tutorial we will walk you through the basics of Clandestine and Covert Online Operations for the purpose of gaining a tactical and strategic advantage over your friends and enemies including your company and organization's competition for the purpose of getting the upper hand in upcoming negotiation acquisition of "know-how" through Talent Management and Technical Collection proactively positioning you your company and organization including your nation as a prominent Offensive Cyber Warfare Power in today's modern Information and Data-driven World.

I'll also provide practical examples in case you're on a possible acquisition spree or might be interested in what would a company or an individual in question do next?

Keep reading!

The main type of Offensive Cyber Warfare Operations include:

Acquisition Spotter – interested in finding new ways to purchase and acquire new Information Security companies and services further expanding your organization's portfolio of services? Keep reading. It should be noted that active monitoring of a company's Competitive Network of Intelligence should become your day one priority. How you can perform better? Do you like going through company Press Releases including Investor Meeting documents and presentations further gaining a Competitive advantage over the company including your competitors? Keep reading. It should be noted that a vast "treasure trove" of Competitive Intelligence information could always be found in a Company's Press Release Section including possible Investor Relations material. Shall we take a moment and use a proper example? Keep reading. Geographical-based events based on publicly obtainable Press Releases could easily plot a company's current and long-term strategy on a map including partnerships and upcoming integration partnerships that could be used to map and keep track of the competition including possible "territory expansion" Sales and Customer Service type of activity and acquisition including possible experience and expertise understanding on what might the individual or organization in question do next in terms of possible company acquisitions and talent and 'know-how" acquisition. Shall we use an example? Are we ready to hit them back? Depends on who you're really dealing with. In this particular case we can use Northrop Grumman's Investor relations "relevations" for the purpose of empowering the U.S DoD and the U.S Intelligence community with the necessary "know-how" to launch and conduct offensive cyber warfare utilizing "restricted payload" further improving an operator's status and observance of cyber space including possible virtual "theater operations". What does really mean? It basically means that one of the major and leading military defense contractors seems to be basically busy utilizing basic OSI model exploitation principles for the purpose of earning additional revenue further positioning itself as a major cyber warfare service provider. What type of tactics techniques and methodologies do they really rely on? It's fairly easy to assume that on the majority of occasions major military defense contracts might be definitely looking forward to "borrowing" technical and strategic "know-how" from a variety of sources including security researchers and the Security Industry in general. A sample "utilization" of this publicly obtainable trade-craft might have to do with utilizing OSINT for capability building including a proactive based "malicious" and classified payload development based on publicly obtainable statistics on some of the most popular devices and browser user-agents currently in use – to further position the defense contractor as a leading provider of proactive classified payload type of provider. What does "classified payload" really mean? It can be best described as a novel use of an outdated and already established methodology courtesy of fellow security researchers and the Security Industry – this time positioned to be further enhanced and utilized by the U.S

Intelligence community. A possible example might be the “borrowing” of tactics utilized and used by some of the market leading Web malware exploitation kits – further enhancing a possible “classified” payload solution with a modified and enhanced payload in a targeted and capability-building capacity. Keep reading. In the second example that we’ll use in this case – we’ll further detail a possible information leak from a possible competitive intelligence type of perspective – namely General Dynamics utilization of Microsoft antivirus and McAfee on proprietary and classified networks further exposing these networks and endpoints to well-known monocultural vulnerabilities and flaws. The relevance? Think twice. With Microsoft’s struggling to perform on the antivirus market segment next to another vendor namely McAfee – it should be noted that these type of information leaks in the face of a possible high-level contractual-based government-type of agreements would eventually do more harm than good in the context of exploiting actual software-based including malware-signatures bypassing in the context of QA (Quality Assurance) and benchmarking applied on behalf of nation-state and rogue cyber actors. What does this constitute? It’s fairly simple to conclude that based on the current state of U.S-based Cyber Warfare and the ongoing departamentalization currently taking place within the U.S Intelligence community the agency in question would be definitely positioned to be proactively exploited and become a main target of notice within the U.S Intelligence community with other agencies and departments seeking to gain access to a fellow agency’s network citing potential monocultural flaws and vulnerabilities.

Trends Acquisition and Monitoring – are you a fan of “Security Trends” and the self-described “Security Predictions” periodically issued to the rest of the Security Industry? With PR departments continuing to “work” the Security Industry on a daily basis – it should be noted that one PR department’s press release can be easily converted in a possible trend and acquisition spotting methodology. What does really mean? It means that prior to go through the very latest and greatest Security Trends – you should definitely keep an eye on the following factors – for instance whether the vendor is piggybacking on a popular buzz-word such as for instance ransomware and whether or not the vendor is actually pitching a new platform solution which should be monitored and potentially researched from a competitive intelligence type of perspective including possible capability-building perspective. Let's use the following examples to demonstrate the case. In the first example we've got several Security Trends type of articles whose value basically lies in a demonstration of basic modern 21st century Security Industry principles known as "*AI and Machine Learning Will Drive Most Cyber Security Efforts* " including possible automation – "*Embracing automation* " in the context of scaling Cyber Security Operations through the utilization of SOC centers including threat intelligence automation and possible orchestration. What does really mean from a potential Cyber Warrior perspective? It means that a potential cyber warrior should definitely try to properly research the platforms in question including basic threat intelligence automation and orchestration principles and either join the job market as a potential competitive prospective or launch a threat intelligence company on their own based on their research. It should be also noted that in terms of AI and Machine Learning potential cyber warriors should avoid falling victim to a particular set of buzz words for the purpose of improving their own market segment competitiveness and possibly either join the job market as a competitive research-based driven prospect or actually launch a company on their own.

Shredding Light on Current Cyber Espionage Attack Vectors – Interested in finding out more the latest technically-relevant cyber espionage attack vectors without the need to get a career in Information Security and Cybercrime Research? Keep reading. It should be noted that potential cyber warriors should definitely stay up-to-date with the latest events in the world of espionage and should definitely continue figuring out proper ways to keep in technical in terms of attack and propagation vectors for the purpose of improving their own market segment competitiveness. Let's use the following example – further demonstrating a common trend namely the re-branding of good old fashioned cyber espionage campaign launched by a sophisticated adversary compared to the today's "modern" APT (advanced persistent threat) which is basically script kiddies utilizing off-the-shelf and most commonly known as proprietary RAT (remote access tool) publicly obtainable at a variety of cybercrime-friendly online communities. What does this mean? It means that basic old-fashioned propagation and infection vectors including the utilization of outdated and already patched client-side based vulnerabilities including the use of newly discovered flaws continues getting utilized this time successfully empowered by the open-source based malicious and fraudulent releases often available as-a-service for the purpose of empowering a new generation of cybercriminals and script kiddies with the necessary tools to launch an offensive cybercrime-friendly attack. How you can perform better? Consider sticking to basic offensive cyber warfare principles and do your research in a variety of areas – most importantly attempt to keep in as technical as possible in the context of empowering your organization with the necessary threat intelligence to stay ahead of current and emerging cyber threats.

Cyber Security Corporate Job and Career Sentiment Research – Do you want to be like the others? Do you want to become a cyber warrior? Keep reading. Based on a general perception that we can all be whatever we really want to be – it should be fairly easy to conclude that a vast majority of readers including Unit-123.org readers can quickly aim to build capabilities based on "information leaks" that can further position the individual as a competitive work-force type of individual successfully acquiring "know-how"? What does constitute an "information leak"? In this example we'll go through a variety of job openings from leading cyber security companies for the purpose of establishing the foundations for a successful "know-how" acquisition and talent management acquisition from the perspective of competitive intelligence perspective. Let's take for instance Cyberint's current Cyber Intelligence Analyst job opening in the context of this example – and further elaborate more on how you should go for interpreting the job career opening in the context of possible application or a possible capability-building. What does this position really mean? Let's take a moment and go through the actual job description – "*managing, monitoring and analyzing US customer's KPIs using CyberInt's unique intelligence platform* ". What does really mean? It means that the individual in question will be definitely looking forward to loosing some of his professional edge for the purpose of digging deep into the vendor’s Threat Intelligence Platform potentially limiting the scope and dimension of his research to a variety of vendor and market-driven research-based topics only. Potential Cyber Warriors interested in becoming vendor-centric type of researchers should definitely consider a “Lone Gunmen” type of career further diving deep into the trenches of cyber warfare and information security in general. Let’s further discuss yet another job proposition from the perspective of cyber warfare capability-building “*Leverages advanced investigative skills to initiate pivoting analysis on Threat Intelligence to identify current impact or proactively process mitigations for defense through security technologies and proactive mitigations including zero-day patching identification and anomalous behavior.* ” meaning that the individual in question should definitely look forward to achieving a decent understanding of zero day exploitation including possible network-based anomaly detection further enhancing his skill set and possibly acquiring new career opportunities. In the last example for this particular case we’ll detail a pretty decent U.S Intelligence community-based career opportunity and will offer a practical insight on how you can perform better. What does this position really mean? It means that a pretty decent portion of your time will go for the common good in this particular case – profiling and analyzing cybercrime groups and campaigns and their online activities.

Social media trends and news discovery – It should be clearly evident that a highly competitive prospective offensive cyber warrior should be on the top of the latest cyber security events and attacks currently taking place. How you can perform better? Consider utilizing basic OSINT concepts including proper news and social media monitoring services to further improve your situational awareness and market segment competitiveness. Let’s use the following examples to further catch up with some of the current events within the shady World of Cyber Warfare. Proper keywords to search for include “NSA” “cyber warfare” “APT” “malware” and “cyber espionage” that would further allow a potential cyber warrior to easily catch up with the latest developments in the world of Cyber Warfare further improving his situational awareness on current and emerging threats. How should a potential cyber warrior proceed in terms of further processing the associated data? Let's use the following example. For instance

SIGINT "assets discovery" analyst – Interested in finding out the latest data including technical know-how in terms of the latest and most active malicious and offensive cyber campaigns? Keep reading. It should be noted that good old fashioned OSINT methodologies including the general availability of RSS readers can come handy in the process of proactively keeping yourself up-to-date in terms of the latest current and emerging cyber threats. Among the key requirements for becoming a SIGINT "assets discovery" analyst in terms of offensive Cyber Warfare perspective is to "follow the trail" not necessarily the money in terms of keeping yourself up to date with the latest developments in terms of a particular offensive and malicious cyber campaign.

Do you want to learn more about clandestine and offensive Cyber Warfare operations including possible OSINT methodology and trade-craft?

Feel free to approach me [email protected]

dancho.danchev

See author's posts

Tags: Cyber Espionage , Cyber Warfare , Cyber Warfare Doctrine , Doctrine , Espionage , Information Warfare , Offensive Cyber Warfare , SIGINT , United States , United States Cyber Warfare Doctrine

Continue Reading

Previous Oops, White House National Cyberspace Strategy Acknowledges Information Warfare Operations Next DoD’s Cyber Strategy – 2018 – Shall We Play a Cyber-Retaliation Game?

France to Wage Offensive Cyber Warfare – Brace Yourselves! – Cyber Intelligence Products – Mobile E-Shop

Did you know that France plans to increase its involvement in the Cyber Warfare space? Brace yourselves! In the most recently released "Paris Call of 12 November 2018 for Trust and Security in Cyberspace " the country raised international concern with its idea to get involved in "offensive" most commonly known as proactive cyber warfare with a newly launched offensive cyber warfare doctrine. How come? Based on an outdated understanding of the current Cyber Warfare market including the U.S Cyber Warfare doctrine directly intersecting with Russia's Iran's and China's – basically a copycat mentality for "communication channel" domination France appears to be wrongly positioning itself as a Cyber Warfare market player that could not only raise someone's eyebrows but could also possibly position the country as a primary target for future and upcoming attacks.

Key points from the Paris Call for Trust and Security in Cyberspace:

increase prevention against and resilience to malicious online activity
protect the accessibility and integrity of the Internet
cooperate in order to prevent interference in electoral processes
work together to combat intellectual property violations via the Internet
prevent the proliferation of malicious online programmes and techniques
improve the security of digital products and services as well as everybody's "cyber hygiene"
clamp down on online mercenary activities and offensive action by non-state actors
work together to strengthen the relevant international standards

It should be noted that major Cyber Warfare powers including the U.S did not get involved in the Paris Call with the exception of U.K., Canada and New Zealand which all signed the agreement. What does the agreement really mean? What does it mean for the U.S and its allies? Keep reading.

From an Information Warfare perspective it should be noted that such widespread calls actually mean to achieve a “media-echo” effect basically re-positioning the country in question as a leading and prominent player in the Cyber Warfare field “without the fuss about it”. Should these calls be avoided and ignored? Definitely.

Would the U.S ultimately position the country as a prominent Cyber Warfare power potentially “listing” the country as a possible source of stolen information and potential wide-spread damage caused by a potential offensive Cyber Warfare campaign launched against the country? Definitely. What France could possibly do in terms of its offensive Cyber Warfare Program? It could definitely aim to piggyback on the U.S Intelligence Community and the Security Industry in terms of establishing a successful SIGINT type of Discovery and “know-how” collection expertise.

Let’s discuss in-depth the key points outlined in the Paris Call for Trust and Security in Cyberspace.

The first point in the Paris Call for Trust and Security in Cyberspace discusses in-depth an eventual response to an increase in “***increase prevention against and resilience to malicious online activity* “** – it can be best described as a desperate call to a wide-spread malicious actor and activity-blocking campaign that aims to harness the Wisdom of Crowds type of malicious actor and campaign blocking-type of activity. Should other countries follow? It should be noted that other countries should definitely avoid to stay away from such type of activity for the purpose of preserving their national sovereignty and for the purpose of not becoming a target themselves. This activity can properly materialize in the context of passive and proactive SIGINT including possible Cyber SIGINT “**assets discovery** ” type of technique and methodology to proactively respond to current and emerging cyber threats.

What the second paragraph – “***protect the accessibility and***

integrity of the Internet " – basically means is a desperate attempt to tackle common Internet flaws known as possible DNS cache poisoning including various attacks on a particular country's Internet infrastructure. What can be done to tackle this common flaws without participating in the agreement? It should be clearly noted that countries interested in protecting their infrastructure should stick to basic Information Security concepts known as the CIA triad namely the protection of the Confidentiality Availability and Integrity of the Information in question relying on basic Information Security principles and methodologies.

The third paragraph – "***cooperate in order to prevent interference in electoral processes*** " – basically means of a way for France on piggyback on the recent U.S based election interference on behalf of Russian hackers utilizing basic Cyber Persona's type of fraudulent and malicious activity in the face of the infamous Guccifer hacker that can be best described as an on purposely generated Cyber Persona that basically "**rebooted its lifecycle** " in a 2.0 fashion courtesy of Pro-Russian hackers that hijacked the Cyber Persona and utilized its popularity and fame for the purpose of spreading a "propaganda message" including the taking of credit for high profile individual and person's hacking attempts and compromised intellectual property.

The fourth paragraph – "***work together to combat intellectual property violations via the Internet*** " can be best described as a desperate attempt to enforce Intellectual Property rights enforcement on the Internet in an attempt to infiltrate and prevent the wide-spread distribution of copyrighted type of content utilizing basic old-school propagation and distribution technologies such as BitTorrent and IRC (Internet Relay Chat) including off-the-shelf P2P file-sharing methodologies.

The fifth paragraph – "***prevent the proliferation of malicious online programmes and techniques*** " – can be best described as futile but basically an upcoming tactic and process on behalf of the French government that will inevitably aim to target a variety of Security Researchers including Forum Communities and Information Repositories that seek to inform educate and spread knowledge on current and emerging cyber threats. Would the French government develop an active or a passive Cyber Operation that aims to disrupt the proliferation of malicious software including popular and off-the-shelf malicious and fraudulent monetization techniques? Largely depends on their current understanding of the process of disrupting and undermining malicious and fraudulent online operations.

The sixth paragraph – "***improve the security of digital products and services as well as everybody's "cyber hygiene"*** " aims to build awareness on the upcoming source code auditing of popular services and products that would ultimately ensure a secure and smooth Internet ecosystem free of security flaws and potential exploitation attempts. In terms of targeting the end user the paragraph will inevitably aim to raise awareness on current and future cyber threats potentially educating tens of thousands of users on basic Cyber Threats the way we know them – malicious software exploits vulnerabilities social media sharing abuse IM (instant messaging) abuse and possible data leak attempts including personal and corporate data leaks.

The seventh paragraph – "***clamp down on online mercenary activities and offensive action by non-state actors*** " aims to raise awareness on the rise and dangers posed by independent contractors that also includes government-based contractors and Security Researchers posing as a possible nation-state type of malicious actors. The paragraph should be considered as an early warning call for hundreds of high profile Security Researchers that should be really putting their efforts into ensuring a proper OPSEC-research based ecosystem proactively protecting themselves and their know-how including Intellectual Property from falling victim into the wrong hands.

The eight paragraph – "***work together to strengthen the relevant international standards*** " aims to build awareness on the country's participation in working on various International Security Standards including the eventual industry-based compliance that might definitely result in improved detection of cyber threats including a possible QA (Quality Assurance) and economies-of-scale type of perspective.

A possible proposal to the French government in terms of the upcoming launch of an offensive cyber warfare doctrine could be the establishment of both defensive an offensive Cyber Warfare unit that could possible ensure both a proactive and reactive response to current and emerging threats facing and somehow threatening the country’s infrastructure. What’s next in terms of a possible offensive Cyber Warfare program could be the direct establishment of a civilian-type of offensive Cyber Warfare community – something that the country might be definitely interested in considering.

The rise of opt-in hacktivism? You wish. Unless the country has the upper hand in a possible civilian-based Hacker and offensive-based Cyber Warfare program – it would be Cyber Warfare basics – back to usual. Piggybacking on civilian offensive Cyber Warfare units for stealing “know-how” is among the key tactics that the country could definitely take into consideration.

What would France do next in terms of an offensive Cyber Warfare program? It could be easily concluded that the country’s current understanding of Offensive Cyber Warfare could wrongly position the country as a primary target launched by nation-state actors including possible rogue actors that could easily find out a way to cripple the country’s infrastructure in case the country doesn’t proactively respond to current and emerging threats. From the logical evolution from passive to active SIGINT and IA (Information Assurance) to CNE (Computer Network Exploitation) it would be noted that sometimes followed the same trail might cause more head-aches than originally anticipated.

Way to go France – but keep in mind that we’ll keep our fingers crossed for an upcoming set of legislative and practical implementation of the proposed efforts.

Recommended reading:

French National Digital Security Strategy French Cyber Security and Defence : An Overview France Cyber Readiness At a Glance

dancho.danchev

See author's posts

Tags: Cyber Warfare , Cyber Warfare Doctrine , Defensive Cyber Warfare , Doctrine , France , France Cyber Warfare Doctrine , French Cyber Warfare Doctrine , Offensive Cyber Warfare , Paris Call for Trust and Security in Cyberspace

Continue Reading

Next UAE – Where Money Pays – Do You Want to be a Cyber Warrior?

Oops, White House National Cyberspace Strategy Acknowledges Information Warfare Operations – Cyber Intelligence Products – Mobile E-Shop

It’s becoming increasingly evident that in a World dominated by Information and Cyber Warfare type of leaks the U.S Intelligence Community should properly seek to account prosecute and track down primary and secondary sources of Information Leaks including the active covert acquisition of technological “know-how” for the purpose of ensuring a proper and smooth-running U.S National Security Policy. Who did steal the secrets to the Kingdom? Check this out.

It appears that the latest White House Cyber Security Strategy – 2018 is wrongly acknowledging the existence and prevalence of Information Warfare tactics including disinformation and trade-craft used by International Partners including rogue and nation-states. What’s the problem?

The United States will use all appropriate tools of national power to expose and counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation. This includes working with foreign government partners as well as the private sector, academia, and civil society to identify, counter, and prevent the use of digital platforms for malign foreign influence operations while respecting civil rights and liberties.

Since when does the White House get involved in Military Affairs to copycat outdated and irrelevant from a U.S Cyber Warfare and Information Operations doctrine-based perspective? Keep reading. Is there a new rise of Military Thinkers that somehow manage to copycat old-school Soviet Union KGB-style type of “know-how” and methodologies for the purpose of re-booting a stegnant military concept known as assymetric warfare which basically intersects with modern Information Warfare? Definitely.

Let’s consider for instance the “Gerasimov Doctrine” which basically aims to shed more light in Russian Information Operations doctrine including a copycat type of initiatives known as disinformation and propaganda. What does the doctrine basically mean? It should be noted that Soviet Union KGB-style techniques and methodologies is similar to applying Sun Tzu’s military thinking and mind-set “know-how” to China’s Unrestricted Warfare doctrine which is basically a copycat thinking based on U.S Military research and analysis papers. Basically a copycat.

It should be also noted that massively investing in new technologies and techniques including “know-how” might definitely raise the eyebrows of the “Old Guard” that basically powers International military forces throughout a vast a modern military thinking and decision-making process. Is this a proper approach to rule and command one of the World’s Most Powerful Armies? Definitely not.

However, it should be also noted that such “innovative” and assymetric modes of thinking could definitely raise the eyebrows of the “Old Guard” leading to what can be best described as a “modern” compartmentalization and departmentalization of certain technques thinking and “know-how” which could greatly damage a military thinker’s long-term reputation within his own country’s military affairs leading to a possible misconduct and Intellectual Property assets damaging including a ruined reputation.

What does the White House National Cyberspace Strategy really mean in terms of Information Warfare operations? It’s a clear indication of a misunderstood trend in terms of implying basic Military Thinking courtesy of a foreign nation within the World’s Leading Cyber Warfare power portfolio of Military and Offensive Cyber Warfare doctrine.

Key points include:

Lead with Objective Collaborative Intelligence – a single-based government-private sector partnership could really pose to be the right track for the purpose of empowering the U.S Intelligence Community with the necessary data information and knowledge to stay ahead of current and emerging cyber threats.

Impose Consequences – the single greatest event that could possibly happen to a rogue state is the direct imposing of consequences in the Virtual Realm that could lead to wide-spread damage and stopping of a target country's critical infrastructure including the waging of Unrestricted and asymmetric type of Information Operations to undermine the country's ability to properly detect the campaign and proactively respond to its initial origin – The U.S Intelligence Community.

Build a Cyber Deterrence Initiative – international cooperation in terms of fighting cybercrime and rogue nation and malicious actor states should be definitely considered as a daily operation within the U.S Intelligence Community. It should be also noted that a proper legislative measure in place could definitely wreak havoc within the U.S Intelligence Community's classified and sensitive Offensive Cyber Warfare projects – "where the left hand doesn't know what the right one is doing" also known as "departmental warfare".

Counter Malign Cyber Influence and Information Operations – the very basic notion of discussing Military Affairs concepts technologies and methodologies within the U.S National Cyberspace Strategy could definitely lead to a negative "media-echo" effect with an unknown number of journalists and researchers joining the bandwagon to properly raise Russia's eyebrows in the currently ongoing Information Warfare and offensive Cyber Warfare driven reality.

dancho.danchev

See author's posts

Tags: Cyber Warfare , Cyber Warfare Doctrine , Information Warfare , Information Warfare Operations , Offensive Cyber Warfare

, Russia , United States , United States Cyber Warfare Doctrine , White House , White House National Cyberspace Strategy

Continue Reading

Next Proactively Digging in the U.S Cyber Warfare Realm – And How You Can Perform Better?

UAE – Where Money Pays – Do You Want to be a Cyber Warrior? – Cyber Intelligence Products – Mobile E-Shop

What can money buy you? An expedited entry into the Cyber Warfare realm – that's for sure. Did you know that throughout the last couple of years the UAE has managed to successfully position itself as a top-dollar Cyber Security Research destination with countless number of U.S based companies looking for ways to make money in the process of outsourcing and offering "know-how"? Keep reading.

Based on a newly published article – it's becoming apparently evident that the UAE is aiming to further position itself as a top-dollar Security and Intelligence contractor destination – with a variety of HR-recruiting type of offers seeking the knowledge and expertise of U.S based Security Researchers companies and Intelligence Analysts including the active "know-how" and methodology acquisition of the purpose of working on currently active Offensive and Defensive Cyber Warfare programs successfully piggybacking on its U.S-based counter-part – the NSA.

What is the UAE up to in terms of Information Security and proactive Cyber Warfare standards and procedures? The most recently released "National Cyber Security Strategy " tackles the following key points:

Prepare and prevent: Aims to raise the minimum protection level of cyber assets and ensure compliance to the UAE's cyber security standards
Respond and recover: Aims to develop incident and response management capabilities and improve threat neutralisation capabilities
Build national capability: Aims to inform and educate the public and workforce about cyber security and promote research in the field
Foster collaboration: Aims to collaborate with international bodies to catalyse cyber security efforts nationally and internationally

Provide national leadership: Aims to develop initiatives to guide the implementation of the National Cyber Security strategy.

It should be noted that proactively investing in Cyber Warfare-based type of research investment might be the right approach to build a national-based type of Cyber Warfare doctrine and strategy. How would leaks be tackled? Who would be responsible for building the technical and HR-driven based “know-how” in terms of building the nation’s Offensive Cyber Warfare program? Keep reading.

Going through the UAE’s Legislative Cybercrime and Information Security based type of legislative material – it should be noted that the country currently possesses a pretty decent understanding of various legislative measures to ensure a proper and smooth Information Security driven type of critical infrastructure further positioning the country as a leading Cyber Warfare power exclusively relying on outsourcing and talent and acquisition “know-how”. How would the UAE’s U.S based counterpart – the NSA respond?

Basically the NSA would properly ensuring a smooth and proper enlisting of the country as an emerging Cyber Warfare power successfully driving its growth through a vast majority of U.S based companies and organizations. What the UAE should keep in mind while positioning itself as a Cyber Warfare “test-bed” for U.S based companies and organizations is that it would be definitely raising the eyebrows of International partners including cyber-espionage groups looking for ways to steal information including the implementation of a successful IA (Information Assurance) policy that would further position the country as a leading offensive “test-bed” for Cyber Warfare practices and “know-how” acquisition.

Do you need to properly position yourself as a Cyber Jihad and R&D research hub? Definitely. What the UAE should keep in mind is that the over-supply of U.S based vendors and organizations interested in investing in the UAE could definitely result in an increase in cyber attacks courtesy of International partners that also includes the NSA looking for ways to obtain access to technical collection including “know-how” expertise including possible leaks.

Are you a U.S based Cyber Security company or an Intelligence Analyst looking for ways to expand the portfolio of services?

Consider the UAE as your primary destination stop.

Related resources:

The State of Cyber (In)security in the United Arab Emirates A Study of Cyber Laws in the United Arab Emirates

dancho.danchev

See author's posts

Tags: Cyber Warfare , Cyber Warfare Doctrine , Offensive Cyber Warfare , UAE , UAE National Cyber Security Strategy , United Arab Emirates , United Arab Emirates National Cyber Strategy

Continue Reading

Previous France to Wage Offensive Cyber Warfare – Brace Yourselves! Next Proactively Digging in the U.S Cyber Warfare Realm – And How You Can Perform Better?