As an adjunct instructor of cyber intelligence (CYB610) and counterintelligence (CYB615) at Utica College, students use live exercises to supplement the academic readings and theories. Recently, the student's in the CYB610 class performed a full open source intelligence (OSINT) targeting, collection, production and analysis of data. The curricula consisted of the standard readings and an overview of OSINT tools and methods anonymity to ensure operational security. The class teaches the students about cybercriminal and foreign intelligence agency methods. The curriculum is designed this way so students not only learn the methods of our enemies (Figure 1), but use these methods as well. The Intelligence Analysis and Production capability provides the ability to merge data and information for the purpose of analyzing, linking, and disseminating timely and actionable intelligence with an emphasis on the larger public safety and the national threat picture. This capability includes the examination of raw data to identify threat and deliver threat estimates, recognize potentially harmful patterns, or connect suspicious links to discern potential indications or warnings. The course delivers not only academic theory but practical, hands-on exercises that support the Comprehensive National Cybersecurity Initiative. The goals of the courses

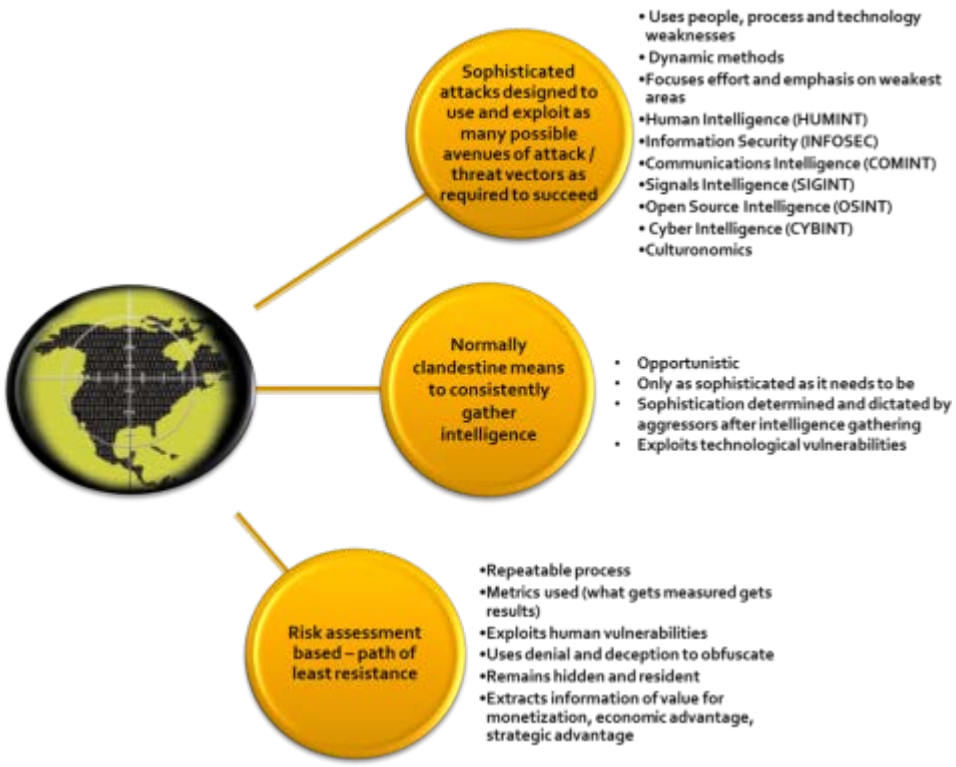

Figure 1 Methods of our enemies

Figure 2 Cyber intelligence Lifecycle

establish and expand cyber intelligence and counterintelligence education and awareness by integrating counterintelligence into cyber operations and analysis.

Cyber Intelligence Lifecycle

The first thing to understand is the cyber intelligence life cycle (Figure 2), which, if you are versed in cyber security, is not much different from the risk assessment process in high level flow. With the target already provided, the students focused on collection and gathering of data, since it is most likely not actionable intelligence during collection. It takes production as a method to organize the data prior to analysis.

Analysis Pitfalls

There are many pitfalls to producing and analyzing data such as personal and professional bias, determining what is deception and misdirection while determining relationships and analyzing various competing theories based upon evidence to construct actionable intelligence. The desired outcome is timely, accurate, and actionable intelligence/information products produced in support of prevention, awareness, deterrence, response, and continuity planning operations.

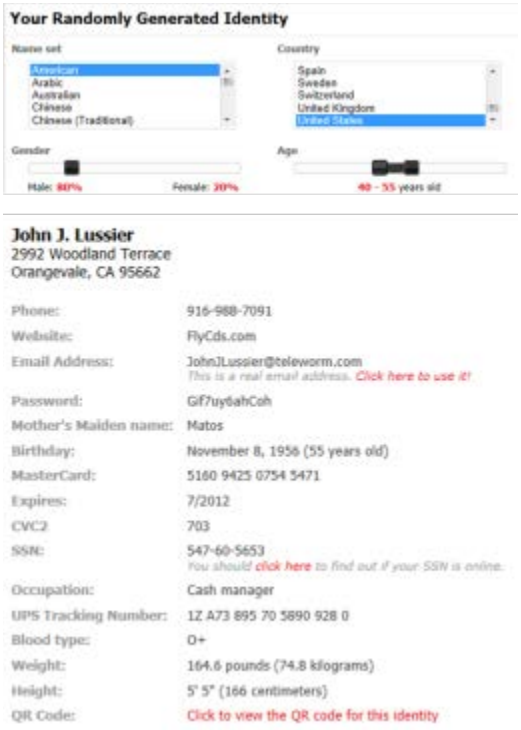

Figure 3 Fake Name Generator

Anonymity

Performing cyber intelligence gathering requires students to anonymize their location of execution as well as their own identity. Denial and deception techniques are required to gather intelligence since student identities must be kept secret. This requires understanding certain tools used to maintain their anonymity. Some of these tools such as Fake Name Generator (Figure 3) assist in creating a cyber persona (sock puppet) to keep your individual identity hidden while others obfuscate your internet protocol address and provide end-to-end encryption:

Table 1 Tools to Anonymize

Virtual machines,	Fanboy's List,
Browsers that are locked down,	Easy List English,
ProXPN,	BetterPrivacy,
Ipredator,	Ghostery,
Tor, CoDeeN	HTTPS-Everwhere,
Vidalia,	ChatZilla,
Tor within Firefox	And commercial tools such as Anonymizer,
Firefox Addins RequestPolicy,	Hide My IP,
AdBlock Plus,	Hide My Ass.

Students need to demonstrate their ability to use these tools prior to proceeding to the collection phase of the cyber intelligence lifecycle. In addition to anonymity of this type, there is the question of sock puppets. Sock puppet development is a critical factor in maintaining anonymity as well as staying true to a personality that has well defined parameters. Some of these parameters are:

First, Middle and Last name
A short bio,
Sex
Age,
Email address(es)
Social networking sites and IDs
City
Country
Profession
Religion
Interests
Connections to other personas you own (a list)
Mother's maiden name
Birthday
Credit card information
Blood type
Height
Weight
Sites where the persona is used
Site roles / responsibilities

Learning your cyber personas is a critical factor to staying within character online. It is much like playing a role in a play or movie only this is real. Maintaining the integrity of your sock puppets take practice and dedication to the craft.

Sample Targeting

In following the cyber intelligence lifecycle, students were provided a possible scenario for targeting.

> The target is considering running for political office. Little is known about this target. Students are cyber intelligence analysts hired by the prospective politicians' campaign organizers to create an intelligence profile of the target. The initial collection effort is to ensure there are no skeletons in the targets past. The secondary collection effort is to produce and analyze the data to determine if the target would make a suitable candidate. The tertiary collection effort is to produce and analyze the data to determine how the targets candidacy could be subverted through a campaign of deception. The tertiary collection and subsequent analysis uses intelligence to deny, deceive, misdirect and deliver misinformation. This is the student's initial foray into cyber counterintelligence.
>
> NOTE: The target for this course is the course adjunct instructor.

The students task provided by their cyber intelligence management:

> Collect any and all available information related to your target's family using open source tools and any legal methods available to you. Gather information about your targets immediate family, brothers, sisters, parents, spouse, spouses family, married status, divorce(s), ages, birthdays, etc. Information to be gathered is birthplace, names, addresses, ages, education, work status/history, religious affiliations, legal/criminal troubles, travel activities, email addresses, phone numbers, pictures, current locations, real estate holdings, etc. Develop site profiles, relationships and metrics. Align relationships based upon frequency of relationships, link and tendency analysis. Identify the open source the tools used, their usefulness and in what situtation where they useful.
>
> Collect any and all available information related to your target's Web 2.0 activities using open source tools and any legal methods available to you. Gather information about your target's activities relative to participation in any Web 2.0 sites such as Facebook, Twitter, LinkedIn and YouTube non-inclusively. Determine where he participates, what groups he participates in and with whom he converses within the Web 2.0 arena. Analyze his use of Web 2.0 and any specific intent.
>
> Collect any and all available information related to your target's potential extremist activity using open source tools and any legal methods available to you. Gather information about target's activities relative to extremism, extremist affiliations, publications, political leanings, foreign affiliations, and associated travel.

Collect any and all available information related to your target relative to his current and past jobs using open source tools and any legal methods available to you. Gather information about your target's activities relative to his profession, any organizations he belongs to or has belonged to, political affiliations, political leanings, associates, speaking engagements, writings of intelligence value, and military service.

Prepare the information in an organized brief. Use HUMINT, OSINT, SIGINT, IMINT, GEOINT, and CYBINT as required. Social engineering is allowed as long as it is legal. Bulleted examples of the requirements are below:

- Adhere to privacy laws. Stay legal!
  - There is nothing illegal about collecting freely available information off the Internet. Cyber personas or sock puppets are not illegal nor is the mining of data posted by people via various Web 2.0 technologies (Facebook, Twitter, YouTube, LinkedIn, etc.).
- Use freely available tools.
- Validate your sources – present credible evidence.
- Demonstrate an ability to extract or collect information from all available sources including relevant online sources, databases and/or systems.
- Prioritize the information based upon the reliability and relevance of the information. Corroborate your sources.
- Analyze the collected information for any potential patterns, links, anomalies, or trends. Use the Analysis of Competing Hypothesis (ACH) tool where applicable.
- Determine if there is any potential criminal and/or a propensity for illegal activity in the target's family past, present or future.
- Determine political leanings with supporting evidence and analysis.

Craft an intelligence brief that provides clear, chronological, relevant, timely, forward-looking, credible and detailed information (quality and reliabilty of resources - cited) on the target. Substantiate the information and line of reasoning. Provide relevant historical information the provides context to the reader. Document your key assumptions in the absence of facts. Present your findings using the two templates (Word and PPT). Define the tools and methods used for gathering/collection. Identify which tools and methods worked best and why. Utilize the capabilities of ACH. Be sure to discuss any potential gaps in the intelligence. Start with your conclusion first in your report using the rest of the report to summarize your arguments.

Analysis of Competing Hypothesis

ACH requires the cyber intelligence analyst to identify and analyze a full set of alternative hypotheses rather than a single most likely conclusion. This ensures that less likely but possible hypotheses receive

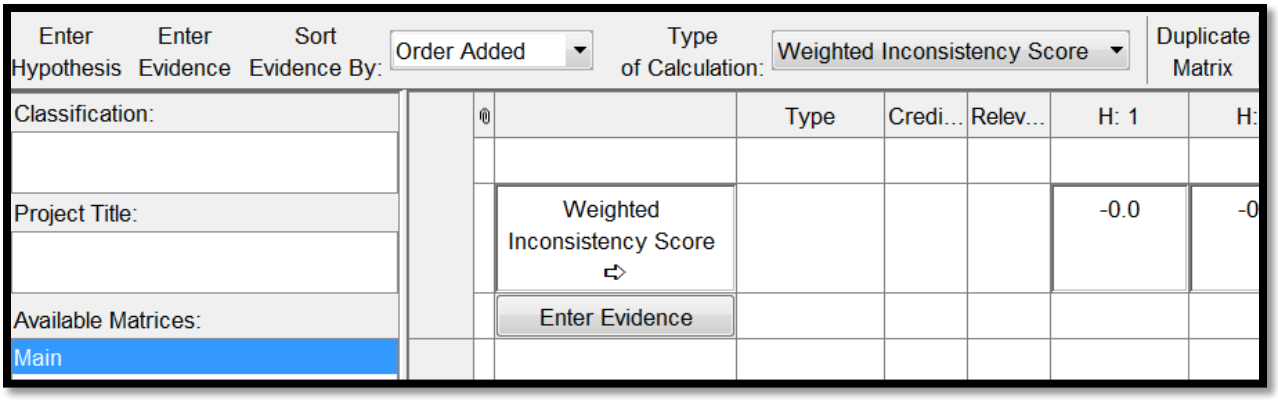

Figure 4 Analysis of Competing Hypothesis

fair treatment. Instead of looking at one hypothesis and weighing the evidence pro and con for that hypothesis, you look at each item of evidence, one at a time, and assess whether that evidence is consistent or inconsistent with each of the hypotheses. This enables the cyber intelligence analyst to determine the "diagnosticity" of the evidence. An item of evidence is diagnostic when it helps the analyst to determine that one or several hypotheses are either more likely or less likely to be true than other hypotheses. An item of evidence that is consistent with all hypotheses has no diagnostic value. The analyst proceeds by trying to refute or eliminate hypotheses, whereas conventional intuitive analysis generally seeks to confirm a favored hypothesis. Evidence without bias is the critical deliverable that drives actionable intelligence using the ACH method.

Suggested OSINT Tools for Usage

The early days of the class require students to become familiar with several OSINT tools. Many of these tools can shorten the cycle time for intelligence gathering while providing insights into potential relationships of value relative to the target. These relationships become sub-targets that may provide data relavant to the tasking. They may be used as methods for social engineering or alignment by

student sock puppets. All tools used and data collected by these tools is documented for applicablity and value to provide other analysts with information on the best tools to use in certain situations. Some of the tools used include:

Table 2 Open Source Tools

http://www.touchgraph.com/ SEO (demo)	http://www.mentionmapp.com/
http://www.silobreaker.com	http://www.spokeo.com
http://www.google.com/squared (now removed)	http://www.pipl.com
http://www.google.com/alerts	http://www.socialcollider.net/
http://newstimeline.googlelabs.com/	http://www.google.com/translate/
http://scholar.google.com/	http://www.topsy.com
http://www.informatica64.com/ FOCA	https://getcocoon.com/
http://www.paterva.com/ (Maltego)	http://www.recordthefuture.com
http://wink.com/	http://PasteLert.com
http://spock.com/	http://addictomatic.com
http://socialmention.com/	http://twoogel.com
http://www.whostalkin.com/	http://knowem.com
http://www.samepoint.com/	robtext
http://www.oneriot.com/	infosniper
http://www.kosmix.com/	omgili
http://www.yacktrack.com	http://openstatussearch.com/
http://tweetscan.com	http://youropenbook.org
http://tweepz.com	

Figure 5 below demonstrates the Java driven demo version of Touchgraph. This is a commercial tool but some functions can be used for OSINT data collection. Each entity in the graph can be doubleclicked to expand with additional relationship trees supported by the URLs. Both the image and the URLs are available for export. Touchgraph provides data on potential sources for more information and additional targets that can support the cyber intelligence lifecycle.

Maltego Community Edition from Paterva (www.paterva.com) is a product from former Cult of the Dead Cow members, now generating products for commercial resale. There is a community version that provides some level of capabilities. Maltego is an OSINT and forensics application that provides the mining and gathering of information as well as the representation of this information in an easy to understand format. Figure 6 demonstrates relationships of followers and those being followed as well as those who retweet Twitter messaging from Treadstone 71. More sources of data and additional targets of opportunity.

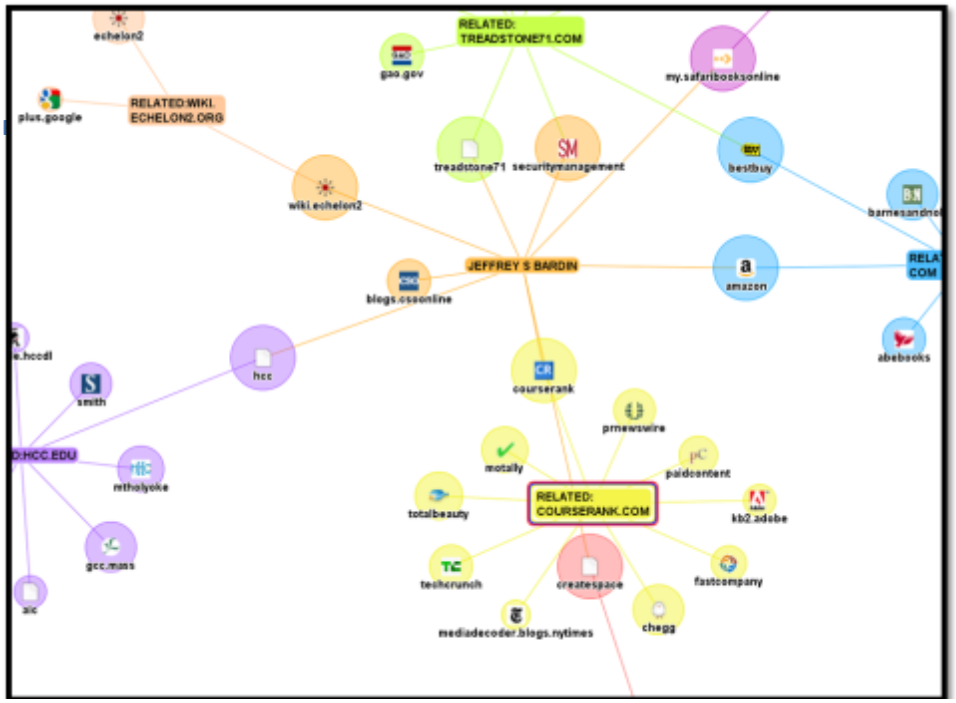

Figure 6 Touchgraph Example

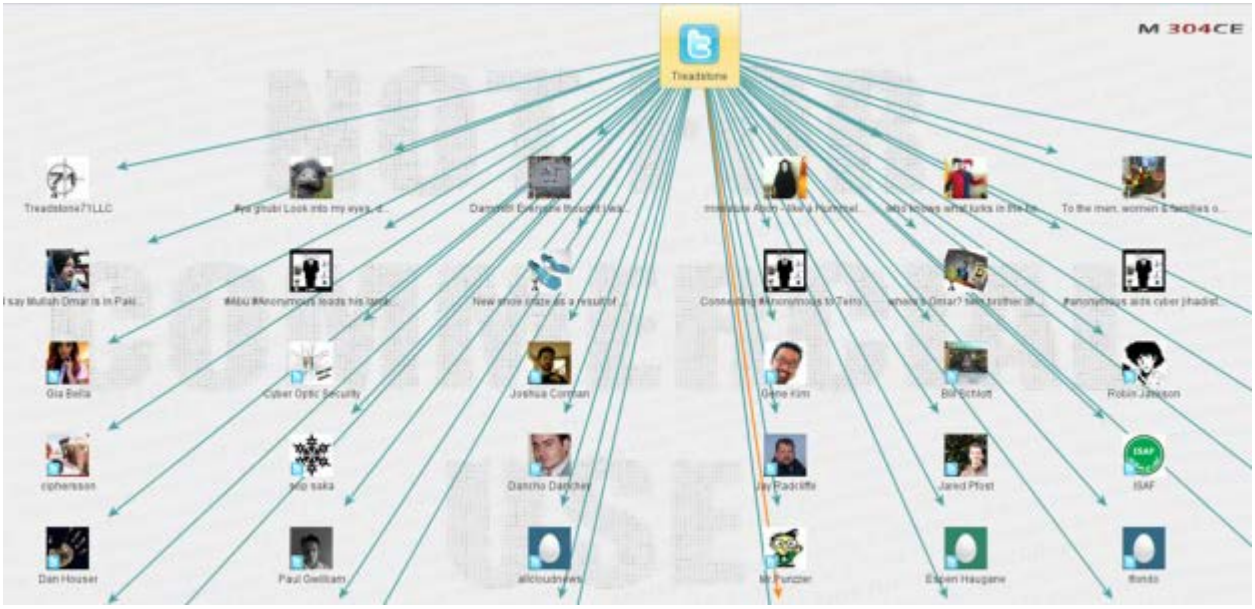

Figure 6 Maltego Community Edition – Twitter Analysis

There are many more tools and methods that effectively used by the students but none more effective than the use of a commercial tool during a 14 day free trial. That tool is Ancestry.com. During the 14-day free trial, one student was able extract birth certificates of every family member of the target including marriage certificates of all who were married. Students may have violated the Ancestry.com terms and conditions by using sock puppets to register but this is not a legal violation but one of potential ethical issue. The question to consider is this: If an adversary such as someone in a foreign intelligence service, uses the same methods and tactics to harvest information about targets in the United States, should it not be an equally viable method for cyber analysts to use the same techniques? Laws are not being broken but ethical struggles can be at the heart of the issue. Suffice to say that the intelligence community and law enforcement requires absolute honesty for job selection and continued employment while denial and deception are taught and required to perform their jobs. The course material at Utica prepares students with practical exercises within the boundaries of the law preparing them for jobs filling gaps in our law enforcement, intelligence community and cybersecurity workforce.

The students continued the data gathering and link analysis by friending unsuspecting target family members through Facebook. The Facebook data collection provided peripheral information about either the target or another family member that followed the information chain, eventually leading to the target in some form or another. Traditional social engineering tactics were employed by a student using a telephone to contact target family members to asking questions to fill in intelligence gaps.

Students find the most interesting part of the exercise to be the possibilities for candidacy subversion.

> Provide methods you would use to create a cyber-based campaign of deception against the target that could potentially discredit the target. Be creative, unique and devious in your methods against the target. Name the method and provide examples per each method.

The following lists a few student's proposed methods:

> An opponent should also target online information about the target. There are many sites regarding the targets experiences and expertise including blogs and interviews. A campaign of misinformation would be best. Flooding the Internet with false and contradicting articles, comments and blog posts would confuse voters and muddy voter perceptions on the candidate. This approach will need to be taken with caution since there is a chance of backfire if a person were to dig deep enough through all the information and find who published it.
>
> The creation of a worm or virus that could be sent to one of the candidate's aides as a disruption method is a possibility. Using a Trojan horse and infecting the opponent's computer systems and shutting them down will delay travel, spreading messages and communication.
>
> The cyber methods used within this deception campaign would ultimately require direct modification, or contribution to the information within the candidate's web presence. The candidate would be targeted in a multi-pronged fashion. The general concept would require undetectable access to the candidate's major accounts. This includes his work and home email accounts, Personal Email (Hotmail, Yahoo, Gmail), LinkedIn, Twitter, and privileged access to the candidate's website. The initial phase would require access to each of these accounts, and undetectable maintenance of access. Once each account was controlled, backdoors would be deployed to the candidate's workstations to ensure that a secondary access method is available in the event the initial access is detected and the candidate attempts to change passwords. In reality, the cyber campaign would be short lived and regarded as an attack, but for someone with a background in security, the impact may be career ending. The most likely vector would be to fingerprint the candidate's workstation operating system, and then use a targeted spear-phishing attack that utilizes a malicious file that is decoyed as a work assignment from a colleague. The following simultaneous actions would be carried out against each account.

Cyber Intelligence and counterintelligence can be an exciting field of endeavor. The National Counterintelligence Executive states that counterintelligence plays a critical role in reversing the benefits that cyber operations afford our adversaries. Cyber intelligence collection and analysis increases our understanding of the adversary and how to defend against them. Counterintelligence operations help identify adversarial tactics reducing the effectiveness of their operations. Collectively, these intelligence and counterintelligence activities increase the cost and risk of our adversaries' operations while reducing their benefits. They play a critical role in enhancing the cybersecurity posture of the United States.

Using the cyber intelligence lifecycle with a plethora of OSINT tools and a bit of devious initiative can be a recipe for disaster for adversaries. Remaining anonymous throughout your collection and gathering efforts is an absolute imperative for cyber intelligence collection. The creation of sock puppets that support one another, strategically placed in social networking sites, Facebook, Twitter, LinkedIn and YouTube can lead to data that becomes actionable information. The most critical skill is learning how to analyze competing hypotheses. Structured analysis based upon evidence and corroboration is a critical factor in the success of your product. The final additive was a taste of cyber counterintelligence focusing on deception, misinformation and perception management. This is data analyzed into actionable intelligence providing recommendations and opportunities to manipulate, direct and misdirect the adversary with standards methods of cyber counterintelligence denial and deception. None of which was taught in CYB 610 (as it is in CYB615). It must be inherent in these students.

Should you wish to pursue a Master's degree receiving academic credit for courses such as the ones described above, see Utica College at http://landing.onlineuticacollege.com/master-cybersecurity/overview-135JE-1547BH.html.

Treadstone 71 also teaches OSINT, Cyber Intelligence, Cyber Counterintelligence, and Cyber Crime courses at the commercial level. See https://www.treadstone71.com/ for more information or via the

Secure Ninja video at http://youtu.be/P8GUoluaekw. Secure Ninja is an authorized provider of Cyber Intelligence courses powered by Treadstone 71 (http://secureninja.com/course/132/Cyber-Intelligence-Training/).

JSB