

News, Resources and Useful Information for the Online Investigative and OSINT Professional from Toddington International Inc.



Toddington International Inc.
Online Research and Intelligence Newsletter
September 2016 EDITION

In This Edition

- [Welcome to the Newsletter](#)
- [Special One-Day Training Programmes: Latest Trends in SOCMINT, OSINT and Cyber-Psychology](#)
- [Oh No! Pokemon Go! - New Security and Safety Issues](#)
- [Resources for the OSINT Professional](#)
- [e-Learning: "Using the Internet as an Investigative Research Tool"](#)
- [Also of Interest to the OSINT Professional](#)

Welcome to the Newsletter

**All New Season of the Hit Television Series "Hunted" Starts
September 22nd**



Filmed over a 28-day period in May of this year, and featuring Toddington International's Julie Clegg and David Toddington, Season 2 of "[Hunted](#)" returns to Channel 4 in the UK on September 22 at 9pm. With £100,000 at stake, this year's "fugitives" are more determined than ever to remain "off the grid" as the Hunters bring to bear new technologies, including helicopters, drones, and dogs in their efforts to track them down.



Effective in its creation of a demanding and pressurized investigative environment, "Hunted" not only accurately represents real-world, high intensity operations, it also pushes the bounds beyond what many investigative and intelligence personnel would be exposed to in typical front-line operations, while introducing a significant number of completely unique stressors.

With Toddington and Clegg serving as the Online Investigative and OSINT specialists, the Hunted HQ team comprised a diverse group of professionals with expertise in Cyber Security/Hacking, Intelligence Analysis, and Behavioral Sciences, from a variety of backgrounds, including law enforcement and military. Caught under an avalanche of an unusually high amount of conflicting data, Hunter HQ personnel found themselves constantly shifting and adapting within an highly dynamic landscape, in which deception was the norm, and creative solutions to highly complex problems were essential for success. With fugitives closely studying each of the 6 episodes from Season 1 (average viewership of 2.2 million per episode), both HQ and ground based Hunters have their work cut out for them in this new season.



With full episodes of *Hunted* available on [4 On Demand](#) for users with UK IP addresses, you can also view the 20 second trailers on [YouTube](#) and follow the series on social media using [#Hunted](#).

Want to acquire some of the unique Online Investigative and OSINT skills developed and used on "Hunted" for yourself? Sign up now for one of our [upcoming one-day seminars](#), enroll in our [acclaimed e-Learning programme](#), or [contact us](#) to enquire about our specialised in-house training courses.

Advanced Intelligence Workshop at the University of Cambridge



Held in conjunction with the International Chamber of Commerce, our 18th bi-annual Advanced Intelligence Workshop at the University of Cambridge was another great success, with public and private sector delegates coming from afar afield as Samoa and Australia, in addition to many parts of the EU in attendance.



Featuring fine dining and a number of social events (*including the welcoming reception in the historic Queens' College dining hall shown above*), 2017 will see the introduction of a specific course focused on compliance with the [European Union 4th Money Laundering Directive](#) and **Online Financial Investigation** techniques on **April 3-5, 2017**, along with an all new **Social Media, Threat**

Assessment and Cyber Psychology focused 3-day curriculum on **September 11-13, 2017**.

With limited seating available, contact [Annette Galloway](#) at +44 20 7423 6960 for more information and to make advanced reservations.

Giving Back to the Community

TII was pleased to provide free training this month to the UK-based charitable organization [Unseen](#), a NGO operating the newly launched [Modern Slavery Helpline and Resource Centre](#), aimed at assisting the victims of modern slavery and helping bring the perpetrators of these crimes to justice.



In addition to Unseen, we were also pleased to volunteer our time with students in a number of high school classrooms providing them with the basic skills to become better consumers of online information, while raising awareness around personal privacy.

e-Learning Graduates

Congratulations to the following students who are among those who have successfully completed the 40 hour [Using the Internet as an Investigative Research Tool™](#) e-Learning program this month:

- Richard Ruiz - Toronto Police Service
- Paige Renout - Xpera Risk Mitigation & Investigations
- Hope McKnight - RBC
- Patrick Vaillancourt
- Alexander Holck - Swedish Competition Authority
- Francis Graf - DPG Consulting Inc.
- Jo Van Lierde - UN Special Tribunal for Lebanon
- Katja von Keitz - DIG Investigations & Security Ltd.

Latest Trends in SOCMINT, OSINT and Cyber-Psychology



LATEST TRENDS IN SOCMINT, OSINT AND CYBER-PSYCHOLOGY

A Specially Priced, All New and Completely Updated One-Day Intensive Seminar

**Sydney - 5th Oct
Singapore - 7th Oct
Hong Kong - 14th Oct
London - 21st Oct**

Your organization is facing an ever-increasing number of internal and external security threats.

As the business and tactical landscape shifts, security professionals, police, and intelligence agencies are now facing never before seen challenges in predicting and identifying a wide range of imminent threats and criminal activities.

Terror groups are posing a significant threat to economic well-being as they seek to advance their political agendas by attacking business premises, and we are seeing a significant shift from coordinated terrorist actions to unpredictable individual assaults. Inspired by online radical discussion forums, “Lone Wolf” terrorists are moving from traditional online platforms to the nefarious “Dark Web” to communicate with like-minded individuals.

Safety and success increasingly depends on the effective use of advanced data mining and search technologies, along with innovative approaches to cyber-psychology, geographic profiling, and social media analytics to generate actionable business and security intelligence.

Join internationally renowned online intelligence expert David Toddington for this unique one-day masterclass and learn about the latest tools and techniques for uncovering, identifying, and analyzing hidden online information that could be critical; not just to public safety, but to business continuity and regulatory compliance.

An excellent introductory session, or a refresher for those who have previously attended our training programs, this new, one-day seminar is being offered on a limited basis at a special introductory price.

This is your opportunity to learn about:

- The latest tools for collecting and analyzing social media intelligence
- New techniques for quickly identifying key associates of targeted online persons of interest
- How the newly emerging discipline of cyber-psychology can give online investigators the upper hand
- Techniques for de-anonymizing and profiling online targets
- Innovative investigative techniques that will improve the efficiency of online research and investigation
- How to maintain operational security in an increasingly challenging online environment
- The latest online anonymity and encryption tools for devices and computers

Who should attend?

- Law Enforcement and Public Safety Professionals
- Regulators and Legal Practitioners
- Security and Compliance Managers and Personnel
- Threat Assessment Professionals
- Fraud and AML Examiners
- Competitive Intelligence Professionals
- Any professional with a “need to know”

Specially Priced at Only \$695 USD

For more information, contact [Kelvin Wong](#) at +852 3978 9918 or [sign up now](#)

Oh No! Pokemon Go! - New Security and Safety Issues



Pixabay

*By Norm Wilhelm, Senior Associate
Toddington International Inc.*

I don't normally write articles that follow recent fads or 'flavour of the month' topics, but the [Pokemon Go](#) game that was released on 6 Jul 2016 is a bit different. With a current estimated following of 130 million people in less than two months, it has proven itself to be quite the global phenomenon, and well worth writing about. At the same time, I don't want to write an article that gets me labelled as a member of 'Team No-Fun'; the derogatory name that some of the younger generation apply to those who write negative articles predicting security breaches and the ruin of society. Instead, I will present some public concerns related to this game, and some perspectives on how it relates to the security industry.

The Phenomenon

For those *very* few persons who aren't sure what this is, Pokemon Go is an augmented reality game that allows players to interact with their geolocation and other players. Using the application on your mobile device, you can see electronic creatures that are spawned by the program into random geographic locations. You can either stay in one place and wait for them to be created (at a rather slow rate) or you can go look for them proactively (thus collecting creatures at a much faster rate). It is actually quite amusing to see these virtual critters sitting on the dashboard of your car, or under the couch in your living room, or wandering across your back yard. They can even spawn on an aircraft

flying at 30,000 ft ASL and on passenger ferries that are crossing large bodies of water. This game is popular with young people between the ages of 8 to 15, but is also popular with those between the ages of 20 and 35 who experienced the first Pokemon craze during the period of 1997-2006.

The Morlocks Arise!

I am sure many parents have already taken note of what has happened to their children who have spent most of the last eight years sitting in front of a computer keyboard, or slouched in dark corners of their households texting and snapchatting on their mobile devices. Like the underground dwellers from the famous H.G. Wells book '[The Time Machine](#)', this army of Pokemon Go players has erupted from their caves in small groups (Poke-packs?), blinking myopically in the sunlight and flexing their atrophied limbs with the sudden need to take physical action. Other than their pasty white skin (from lack of exposure to sunlight), these dedicated players can sometimes be identified by their lack of attention to their environment.

Caution: Poke-Player Crossing

There are a large number of people who do not play this game, and it is this majority that is being required to take defensive action against potential accident and/or injury. In addition to the already acknowledged problem of distracted driving, we now have an increasing number of reports regarding people engaging in 'distracted walking'. Many of these Pokemon Go players will be distracted by the game in the same way as a person walking down the street reading a book. In the past, drivers kept an eye out for kids playing street hockey or kicking their soccer ball over the fence of a school field. All drivers in future will need to be cautious of 'Poke-players' who seem to have forgotten their lessons about how to cross the street, darting across the roads in pursuit of their elusive e-critters.

Poke-Mobs and Time Theft

This gaming phenomenon is not limited to just youths under the age of eighteen. There are quite a few adults between the ages of 20 and 30 experiencing the nostalgia of a card game and TV series they watched as a kid. These enthusiasts are now in adult work environments, and are getting distracted from their daily tasks by rare spawning e-critters that appear on the streets several stories below. In one story I was entertained by an adult employee wrestled with the dilemma of continuing his assigned work or taking a few minutes to race down ten stories to street level in order to capture a rare Pokemon creature he had just identified on his device. Succumbing to temptation, he was soon on street level where he become part of a crowd of over two hundred office workers and passers-by, all

trying to capture the same creature. The event was essentially recreating the 'flash mobs' that we saw back in 2009. In response, employers may need to expand their employee guidelines in regards to employee participation in augmented reality games during working hours. This may also affect loss-prevention workers who know that there are always some criminal elements willing to take advantage of the distractions caused by large concentrations of people.

The Perception of Suspicious Activity...

For those engaged as security industry workers, whether as police officers or private security, this game is causing some re-adjustment as to how we perceive stereotypical suspicious behavior. For example, that group of young people by that building over there would normally be considered worth talking to, especially under darkness of night in an area known for youth related problems. Is it vandalism? Is someone being bullied? A gang fight? A drug deal? Possibly no to all of these; it's a group of Pokemon players battling for possession of a 'gym'. They see nothing wrong with their law-abiding behavior, and there really is nothing wrong with what they are doing, as long as they are on public property.

... And Illegal Activity By Players

But not all players are being law-abiding and staying on public property. There are an increasing number of law suits being filed at courts across North America as property owners object to a parade of Pokemon Go players hopping their fences in pursuit of electronic quarry, or trying to access a Pokemon 'gym' (where the player can train and increase the power of the creatures they capture) that have been randomly positioned across the continent by the gaming program. Examples of badly placed gym locations include proximity to [outlaw motorcycle gang clubhouses](#), construction sites, condemned buildings and fenced-in private property of all types. In such cases, while trespassing is clearly the fault of the player and not the property owner, all property owners who have security concerns are advised to check that no augmented reality sites are being set up on or near their property. Court cases all already in progress that will determine how these can be reported and removed.

Increased Activity And Social Interaction

Granted, some enthusiastic players are having problems adjusting to the 'real world', with far too many seeming to have forgotten their lessons of (i.e.) about staying off of roads, along with other childhood safety rules. But these appear to be the exceptions rather than the rule. The Pokemon Go game as a whole is an industry model of how to develop participant motivation, and has resulted in

thousands of youth being more active and interactive than ever before. More important to realize is that it is the first game of its kind, and the gaming industry (like any other) always follows success. Over the next twelve months we can expect similar games to be developed and released based on the same gaming principles as this one.

Some Investigative Avenues

Those of us who do investigations related to insurance claims might see a few advantages in this popular game. Learning that a claimant is playing this particular game can indicate that they are physically active and interacting with other people, leading to new avenues of inquiry. In turn, if someone becomes suspicious of why a security professional is conducting surveillance in a particular area, they could possibly attribute their actions with a claim they are playing Pokemon Go (and actually have the app installed on their device!).

The blunt truth is that a significant number of young people understand their devices, information exposure, and security risks better than many of their elders and are not interested in reading articles written by members of 'Team No-Fun'; aka any negative-toned article written by practitioners in the security industry. The stories seen in the news over the past few weeks are not typical of all players of this game or games like it. Times change and new games like this are reminders that new technology will always cause some sort of social upheaval. There was a time when cell phones were banned from being carried by students in schools. Eventually they became socially accepted (with a few new rules from supervisory bodies) and now a significant number of students carry their devices into classes. In a similar manner, this gaming phenomenon, its side-effects, and social behavior consequences are going to reach a state of balance.

Drawing a line in the sand is not going to stop this gaming phenomenon; it will require an accommodation between the two sides, requiring some acceptance of strange behavior from non-players, and a reduction in extreme behavior by the ardent players.



Norm Wilhelm is an investigator, intelligence analyst and instructor with Toddington International and has over 20 years of experience in open source intelligence and online investigations. He is a highly decorated and accomplished former member of Canadian military intelligence, who later worked in the human resource management industry and then at one of Canada's largest private investigation companies, specializing in online investigations and research. The majority of his work over the past nine years has supported workplace investigations, threat assessments,

insurance fraud, class action suits, and family law. In November 2013, he was recognized by the Supreme Court of British Columbia as an expert in open source intelligence and online investigations.

Sponsored Message



**Enhance your situational
awareness with real-time
event monitoring**



Searching with Echosec allows you to filter through the noise of over *2 billion people* on social media and find what's important. **See live posts, as they happen, from around the world.**

START SEARCHING NOW

Resources for the OSINT Professional



<https://www.howsmyssl.com> - Allows you to easily check the quality and security of your secure web connection

<http://epic.org/privacy/tools.html> - EPIC Online Guide to Practical Privacy Tools: A good collection of tools and resources to protect your privacy

<http://BBB.org/scamtracker> - Great new tool from BBB that geographically indexes current and emerging scams and frauds

<http://www.watchoutinvestors.com> - Search for regulatory or disciplinary actions against corporate entities

<https://investigativedashboard.org> - An excellent research portal for investigators, intelligence professionals and investigative journalists alike

<https://oldgeekjobs.com> - Job postings board for those over 30 and a move to overcome age discrimination in Silicone Valley tech industry

<https://geoguessr.com> - Geo-discovery game: Players figure out a global location using only clues visible in randomized Street View images

<http://www.gpsvisualizer.com/geocode> - Find the latitude and longitude of a street address using this GPS Geocoder

<http://onemilliontweetmap.com> - Interesting site showing the world's last 1 million tweets plotted on a global map

<https://wagle.net> - Wireless Geographic Plotting Engine plotting Wifi hotspots on maps

<https://www.abine.com/optouts.php> - "How to Protect Your Data and Remove Personal Information from the Internet for Free"

<http://current.ly> - Twitter monitoring and search tool

<https://www.diigo.com> - Social bookmarking site for saving online resources

<http://worldc.am> - Global Instagram photo search by location

<https://vine.co> - Vine social network video search

<https://connectonline.asic.gov.au> - Australia Securities and Investments Commission company search

<http://www.collinsdictionary.com/translator> - Online translator, also available as a mobile app

<http://findgram.com> - Instagram search tool; search by hashtag or user

<http://www.fec.gov/disclosure.shtml> - US campaign finance reports and data, searchable by candidate

Want more? Visit our continually updated, [FREE Online Research Resources Page](#) featuring hundreds of links, cheat sheets, investigative guidelines and more!



Comprehensive E-Learning Program

Using the Internet as an Investigative Research Tool™



e-Learning: "Using the Internet as an Investigative Research Tool"

Take your Online Research and Intelligence Skills to New Levels

The most comprehensive and up-to-date Internet Research e-Learning program available anywhere, "Using the Internet as an Investigative Research Tool" is designed to enable investigators, researchers and intelligence personnel to find better online information, in less time, at less cost, with less risk".

For a fraction of the cost of a classroom based training course, our flexible and interactive virtual classroom environment allows candidates to progress at their own pace and competency level with a qualified personal instructor on hand at all times to ensure success. Initially launched in 1998, this highly acclaimed and continually updated online course has been successfully completed by over six thousand investigators and knowledge workers around the world.

As a HRSDC certified educational institution, TII provides Canadian students with a T2202 Tax Receipt and a Certificate of Completion from the Ontario Police College.

Enrollment takes only a few moments; online credit card payments are accepted, ***group discounts and licensing options are available for five or more registrants.***

Bonus: Tuition fee includes a one-year subscription to the newly revised and updated TII Premium Resource Knowledge Base, a premium resource of some 4,000 deep web resources

and sites (an additional \$299 value)

Visit the [TII e-Learning page](#) to find out more and instantly register, or [contact us](#) directly with any questions

Also of Interest to the OSINT Professional

[A SysAdmin's brief DNS misconfiguration and a glimpse into the DPRK Hermit Kingdom's strange version of the Web](#)

[Google backs off on previously announced Allo privacy feature: The app will log conversations by default after all](#)

[Bots are waging a passive-aggressive war on Wikipedia](#)

[“How Spy Tech Firms Let Governments See Everything on a Smartphone”](#)

[Machines engaging in data analysis without human intervention — what could possibly go wrong?](#)

[Time to change passwords: Some 68,648,009 Dropbox account details hacked in 2012 breach now coming to light](#)

[New system doubles number of points mapped to facial features to improve the system's ability to match photographs](#)

[With up to 100 ECUs and more than 100 million lines of code, vehicles today present massive attack surface](#)

[Wireless Emergency Alerts \(WEA\), geographically targeted text messages alerting of imminent threats in a given area](#)

[Not always as easy as you may think: "How to Digitally Erase All Your Stuff When You Quit Your Job"](#)

[FB has been changing privacy options again with default option being for you to be oversharing your details](#)

[“How One Journalist Uses Social Media to Get Inside the Minds of ISIS”](#)

["Data to Go" from Cifas UK, an excellent demonstration of how a single Facebook "like" can reveal so much about you](#)

[Government group recommends against using text messages to secure your passwords](#)

[92% of UK businesses fail to encrypt over 75% of their sensitive & confidential data in the cloud](#)

[One of the most overlooked search engines out there \(with some solid privacy features\)](#)

[UAE introduces law banning the use of VPNs to try to avoid paying for expensive VOIP services](#)

[follow on Twitter](#) | [friend on Facebook](#) | [forward to a friend](#)

Copyright © 2016 Toddington International Inc., All rights reserved.

[unsubscribe from this list](#) | [update subscription preferences](#)