TODDINGTON INTERNATIONAL INC.

Knowledge Powered by Intelligence™

405C LE-HC

Hacktivism and Cyber-Warfare

Law Enforcement / Defense Sector Services

In hacktivism and cyber-warfare, critical information, assets and infrastructure are attacked, disrupted or compromised in an effort to conduct espionage, or to sabotage or destabilize the political or military efforts of a nation or state.

With the developed world's reliance on electronic data transmission and complex computer systems that control everything from water purification to global financial oversight, the damage that can be caused by cyber attacks is immeasurable. The scope and scale of these potential vulnerabilities is matched by the speed with which many of these systems could be disabled or disrupted, making the protection of our electronic and digital data and systems a significant global priority.

In 2010, the STUXNET worm compromised computer system controls that were used to enrich Uranium and, in turn, reportedly destroyed nearly 1,000 centrifuges. In 2012, the SHAMOON worm, believed to be a copycat of STUXNET, did more than just compromise these computer systems - it destroyed more than 30,000 of them, making it one of the largest attacks on a private sector system in history.

These attacks reinforce the intention to cause physical destruction by virtual means, resulting in significant financial cost. As a direct result of cyber attacks, the United States has been forced to close two nuclear plants, costing $1 million per day to divert power from other parts of the energy grid.

Our comprehensive training explores the causes and effects of hacktivism and cyber-warfare at local, domestic and international levels, and provides comprehensive instruction on the detection and identification of system vulnerabilities, and the isolation, monitoring and disruption of cyber attacks on critical information systems.

COURSE OPTIONS

Hacktivism and Cyber-Warfare - Basic 1 Day

- Examining and Detecting Open Source Vulnerabilities
- Online Reputation Management
- Basic and Advanced Cross-Platform Search
- Digital and Physical Privacy and Security
- Defensive and Predictive Data Tactics

Hacktivism and Cyber-Warfare - Advanced 2 Days

- Geo-Location and Linking of People, Places and Things
- De-Anonymization and Identity Disambiguation
- Known and Unknown Threat Assessments
- Secondary Targets, Associations and Predictive Pattern Analysis
- Targeted Surveillance and Monitoring Techniques

About TII:

With a global client base ranging from government agencies to members of the Fortune 500, **Toddington International Inc. ("TII")** has been enabling its customers to find and use online information more effectively since 1997.

Backed by over a decade and a half of experience providing advanced Internet intelligence services to a range of law enforcement agencies, in addition to private sector clients in the financial services, petrochemical, pharmaceutical and manufacturing industries, TII develops and delivers comprehensive, highly acclaimed class-room-based and e-learning programs that enable frontline investigative and research professionals to **find better online information, in less time, at less cost, with less risk™**.

Our team of trusted associates includes highly qualified investigators, intelligence analysts, psychologists, educators, legal practitioners and other professionals, all of whom maintain the highest standards of integrity.

TODDINGTON INTERNATIONAL INC.
The Industry Leaders
+1.604.468.9222
training@toddington.com
www.TODDINGTON.com