United Nations
Interregional Crime and Justice
Research Institute

Hackers Profiling Project V2.0 (HPP V2.0)

What is it?

The project is envisioned as a continuation of our Hackers Profiling Project, commenced in 2004, which sought to identify the characteristics of the independent hackers that dominated the cybercriminal scene of that time. Once published, the project was acclaimed by law enforcement agencies, judges and policy makers worldwide who praised it for providing an understanding of the underground cyber world in criminological terms familiar to them.

Like its predecessor, HHP V2.0 seeks to provide law enforcement agencies, judicial bodies and policy makers with a tool investigate and analyze cyber-attacks that bridges conventional criminal justice with the peculiarities of the cyber-underground. However it distinguishes itself by focusing on the characteristics of the organizations that engage in cybercriminal activities instead of the individuals themselves. Therefore the study focuses on the demystification of the terms "hacktivists", "organized cybercrime" and "terrorism" by analyzing openly sourced literature and intelligence derived from strategic partnerships with law enforcement agencies, government bodies, private institutions and the media.

In its conclusion the project will expose a variety of profiles for groups that commit cyber-attacks by outlining their common and distinguishing traits.

Why it is relevant?

These profiling methodology will provide the end user with a starting point for his/her own cybercriminal investigations; he/she will be able to confront the facts of his/her case with the templates in HPP and be able to identify the components of the case in a speedier and more accurate way.

With a focus on the public sector, it could prove a useful tool for:

-**Law Enforcement Agents**-that can use it as a launching platform to identify the initial parameters of their investigation.
-**Judiciary and Legal Sector**-that can use to evaluate the stance of actors involved in cyber cases and gain insight into the potential elements of mens rea which govern acts in cyberspace
-**Policy Makers and Governmental Bodies**- that can use it as a non-bias and accurate account of the modus operandi of contemporary threat agents.

United Nations
Interregional Crime and Justice Research Institute
Viale Maestri del Lavoro, 10 - 10127 Turin, Italy
Telephone: (+39) 011 653 71 11 - Telefax: (+39) 011 631 33 68
E-Mail: unicri@unicri.it - Web site: www.unicri.it

Stages of the Project

1- Literature Review
2- Data Collection
3- Data Analysis
4- Assemblage, critical review and peer editing
5- Dissemination

UNICRI's projects achieve significant visibility throughout the international community due to the institute's outstanding global network of public and private institutions.

HHP's distribution at international conferences, lectures and courses will amplify the scope of its impact and render it a readily available tool for institutions and individuals across the globe.

UNICRI is currently working on the first phase of HPPV(2.0), as it is a project based institute, it is crucial that it ensures funding before being able to progress to the following stages of the project.

How We Plan On Protecting the Data We Receive

Depending on the type of data subject to the exchange, we will ensure that both the transition and storage phases are met with adequate security measures.

Though invariably the nature of the arrangements will depend on the nature of the exchange UNICRI will ensure that the measures in place fulfill the criteria outlined by its partners.

HPPV(2.0) Sponsorship Benefits

-Access to the extensive UN network
-Periodic updates of the ongoing research
-The cooperation and support of all the institutions that participated in the first HPP
-Participation to seminars and workshops organized to gather experiences and perspectives from policy makers and law enforcement agencies world wide.

UNICRI's Synergies and Existing Support for HPP

We have over a decade of experience in dealing with matters of organized crime in all its different facades. This has enabled us to create a unique network of contacts and places us in the ideal position to bridge traditional criminological approaches with the novel investigative methodologies required to tackle cyber-crime calls.

The primary contacts that have already expressed an interest in supporting HPPV(2.0) are, among others, Europol, Interpol, NATO, National Law Enforcement Agencies (Italy, Turkey and Holland), IGaK Berlin, Channel 4 (UK), Wired and Mediaset (IT).

More about UNICRI

UNICRI operates a unique strategic response to securing cyberspace which could benefit from collaboration on several fronts, including our ongoing research in:

- Cyberwar and Cyberterrorism
- Organised Crime and Cybercrime
- The Impact of Cybercrime on Business and Finance
- Child Online Protection
- Criminal Use of Social Networks
- Developing a Harmonised Methodology for Cybercrime Research and Investigation

Each of the above proposals, including HPP, was conceived independently from specific call for proposals. Thus, every proposal listed can be further focused and targeted, in terms of capacity, deliverables, budget, timeframe, and geographical scope, according to the unique necessity of the individual call and the subsequent consortium.

The institute is internationally renowned for the quality of its research and can count on the support of the whole UN System and first class experts in virtually every area of organized crime. Alongside cybercrime the other areas of focus include:

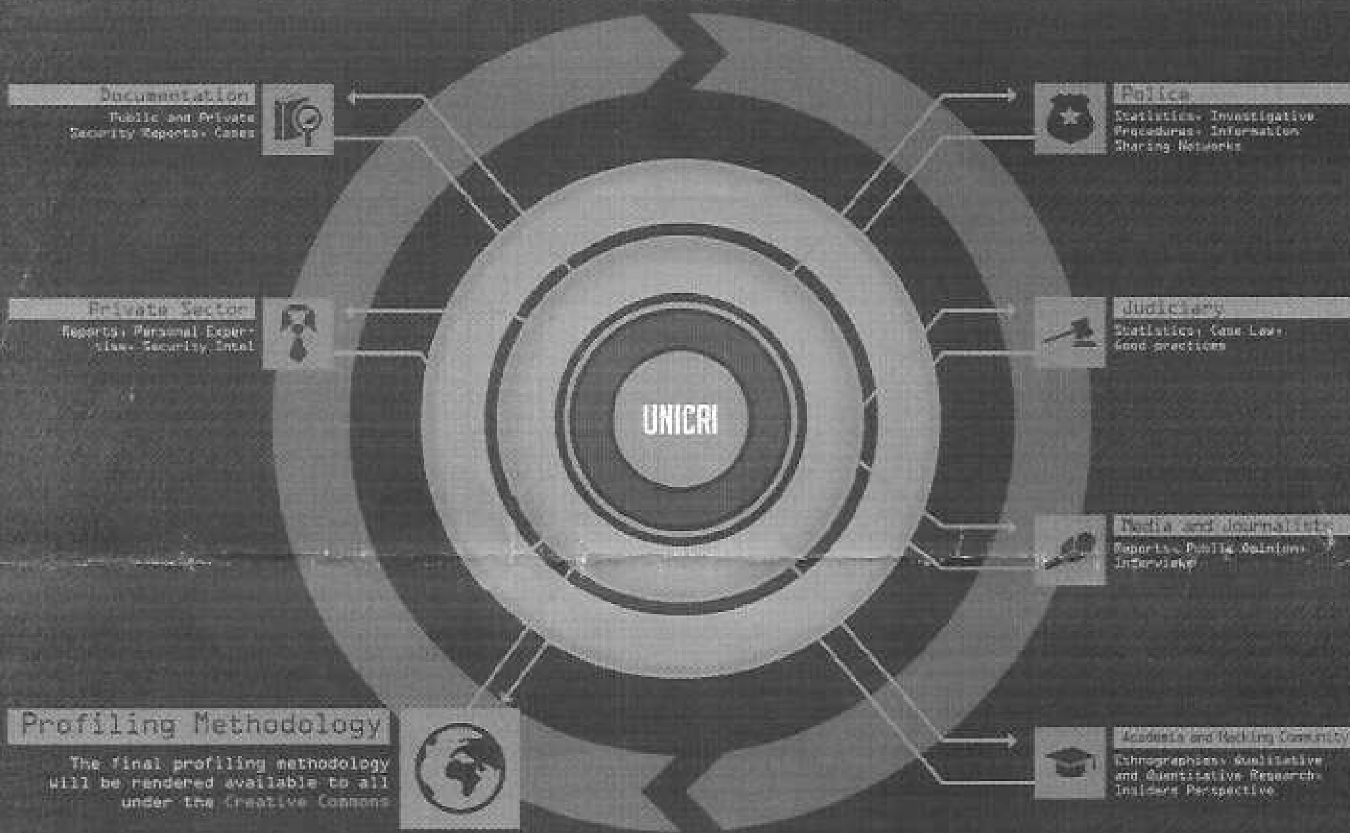
- Environmental Crimes
- Counterfeiting
- Profiling and Data Protection
- Chemical Biological Nuclear and Radioactive Weaponry
- Terrorism

This breadth of knowledge and ongoing research enables us to produce interdisciplinary research of the highest standard and to offer our partners an unbiased perspective that accounts for the latest developments and foremost advances of criminal justice.

HPP V2.0 Hackers Profiling Project V2.0

It is becoming increasingly difficult to pin-point the culprits of cyberviolations. The majority of cyber attacks can be attributed to Organized Criminal Groups, Governments and Hacktivists. However, such a breakdown fails to account for the morphing definitions of the terms 'organized crime', 'government' and 'hacktivism' in cyberspace. The structure of Organized Criminal groups, hacktivist cohorts and the relationships between governments and economic forces, are evolving so quickly that the titles 'Organized Crime', 'Hacktivism' and 'Government' are meaningless in terms of cybersecurity. What is needed is a study that looks at the specific characteristics of each group that commits these crimes. Building upon HPP V1.0, which described the features of individual hackers, this project focuses on identifying the traits of Organized Cybercriminal groups, State sponsored attackers and Hacktivists that constitute cyberthreats.

For further details contact:
bosco@unicri.it



PHASES

Our website: www.unicri.it/special_topics/cyber_threats

#01 Documentation

Collection and desk review of all gathered material relating to cyberthreat agents.

#02 Intel

Collection of data feeds from worldwide law enforcement agencies, academia, companies and experts. This phase will benefit greatly from the extensive network of contacts that UNICRI has built over the past decade.

#03 Analysis

Analysis and correlation of the data gathered with the material reviewed in the first phase.

#04 Production

Production of the HPP V2.0 Methodology, tested against an extensive field peer-review.

#05 Dissemination

ISECOM and UNICRI will collaborate to render its findings available to all under the Creative Commons.

HPP V.2.0 will provide law enforcement agencies, governments, private and public sector forces with a tool to assess, prevent and counter cyber-threats.

unicri