

# Chapter 70

## A Socio–Technical Perspective on Threat Intelligence Informed Digital Forensic Readiness

**Nikolaos Serketzis**

*Aristotle University of Thessaloniki, Thessaloniki, Greece*

**Vasilios Katos**

*Bournemouth University, Poole, UK*

**Christos Ilioudis**

*Alexander Technological Educational Institute of Thessaloniki, Thessaloniki, Greece*

**Dimitrios Baltatzis**

*International Hellenic University, Thessaloniki, Greece*

**George J Pangalos**

*Aristotle University of Thessaloniki, Thessaloniki, Greece*

### ABSTRACT

*In this article, a DFR framework is proposed focusing on the prioritization, triaging and selection of Indicators of Compromise (IoC) to be used when investigating of security incidents. A core component of the framework is the contextualization of the IoCs to the underlying organization, which can be achieved with the use of clustering and classification algorithms and a local IoC database.*

### 1. INTRODUCTION

Digital forensics dates over four decades. Unlike other forensic science disciplines, digital forensics faces the challenge to operate in a problem domain where the subject of study evolves in an intermittent, non-linear fashion. For instance, a routine, nightly update of the software or introduction of new hardware may

DOI: 10.4018/978-1-7998-2466-4.ch070

substantially change the behavior of the underlying system, requiring a significant revision of the digital forensics acquisition and analysis processes. Consider for example the case of evolution of traditional hard disks to solid state disk (SSD) technology. The way the latter operate invalidate many key assumptions under which forensic acquisition and investigation of disks is performed (Bednar & Katos, 2011).

Moreover, the proliferation of heterogeneous networked devices and the amount of data they are capable of producing – as captured under the terms IoT and Big Data respectively – has exacerbated the problems and challenges of digital forensics. As such, digital forensic readiness (DFR) has become a critical function of the organization's security processes and achieving efficient DFR has become a high priority. Research in digital forensics has primarily evolved through a responsive, practitioner-based attitude. The relevant literature on digital forensics is dominated by techniques and practical approaches for obtaining and analyzing data in specific contexts and system configurations. When it comes to considering DFR approaches, the level of abstraction is high causing a void and eventually a disjoint between DFR and digital forensic investigations. Most DFR research publications are limited to describing high-level and generic steps, whereas contextualization is mostly absent. This work aims to bridge the gap by proposing a framework for a closer coupling between DFR, forensics and incident response for addressing Advanced Persistent Threats. We argue that inevitably, the prioritisation and contextualisation of the Indicators of Compromise is a sociotechnical challenge, since ultimately the forensic analyst needs to leverage automated tools to support their cyber situational awareness posture. That is, following a detection of a security breach, the threat related information needs to be quickly accessed, correlated and highlighted to allow the forensic analyst to triage, prioritise and guide their investigation in an effective manner.

The rest of the paper is structured as follows. Section 2 presents the relevant literature. In Section 3 our approach is developed. Section 4 outlines a typical APT scenario to be used as a vehicle to showcase our approach, and section 5 summarises the conclusions.

## **2. RELATED WORKS**

In a seminal paper, Hutchins et al. (Hutchins, Cloppert, & Amin, 2011) proposed an approach for studying and improving incident response against APTs. They introduced a cyber kill chain which identifies a path comprised of 7 discrete and sequential phases an attacker follows to meet their adversarial goals. From a digital forensics perspective, the kill chain is particularly helpful in highlighting the following:

- Every successful (to the attacker) phase is a direct consequence of the respective security control failures.
- Detecting the security breach early in the chain infers low impact and potential damage.
- Late detection of the security breach implies that there are more security failures. Hence the scope of the digital forensic artifact collection is wider.

For the remainder of this section, the relevant subtopics that will enable the key chain to leverage the proposed DFR framework are presented.

10 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/a-socio-technical-perspective-on-threat-intelligence-informed-digital-forensic-readiness/251486](http://www.igi-global.com/chapter/a-socio-technical-perspective-on-threat-intelligence-informed-digital-forensic-readiness/251486)

## Related Content

---

### From "Cyberterrorism" to "Online Radicalism"

Maura Conway (2014). *Exchanging Terrorism Oxygen for Media Airwaves: The Age of Terroredia* (pp. 198-217).

[www.irma-international.org/chapter/from-cyberterrorism-to-online-radicalism/106164](http://www.irma-international.org/chapter/from-cyberterrorism-to-online-radicalism/106164)

### A South African Legal Perspective on the Regulation of Net Neutrality and Its Implications for Cyber-Security and Cyber-Warfare

Trishana Ramluckan (2020). *International Journal of Cyber Warfare and Terrorism* (pp. 36-47).

[www.irma-international.org/article/a-south-african-legal-perspective-on-the-regulation-of-net-neutrality-and-its-implications-for-cyber-security-and-cyber-warfare/263025](http://www.irma-international.org/article/a-south-african-legal-perspective-on-the-regulation-of-net-neutrality-and-its-implications-for-cyber-security-and-cyber-warfare/263025)

### Information Security Culture: Towards an Instrument for Assessing Security Management Practices

Joo S. Lim, Sean B. Maynard, Atif Ahmad and Shanton Chang (2015). *International Journal of Cyber Warfare and Terrorism* (pp. 31-52).

[www.irma-international.org/article/information-security-culture/138277](http://www.irma-international.org/article/information-security-culture/138277)

### Web Defacements and Semantic Attacks

Lech J. Janczewski and Andrew M. Colarik (2005). *Managerial Guide for Handling Cyber-Terrorism and Information Warfare* (pp. 97-105).

[www.irma-international.org/chapter/web-defacements-semantic-attacks/25670](http://www.irma-international.org/chapter/web-defacements-semantic-attacks/25670)

### The Winds of Change in World Politics and the Impact on Cyber Stability

Virginia Greiman (2019). *International Journal of Cyber Warfare and Terrorism* (pp. 27-43).

[www.irma-international.org/article/the-winds-of-change-in-world-politics-and-the-impact-on-cyber-stability/246332](http://www.irma-international.org/article/the-winds-of-change-in-world-politics-and-the-impact-on-cyber-stability/246332)