# Digital Forensics in a Cyber Warfare Context

Alessandro Guarino

StudioAG – ICT Consulting & Engineering
e-mail a.guarino@studioag.eu

## Abstract

The paper explores the application of digital forensics techniques to cyber warfare scenarios. A common accepted taxonomy for digital forensics (and anti-forensics) activities, techniques, procedures and work flows does not yet exist but guidelines and even international standards have given the field a framework: this paper explores how digital forensics can be logically framed in the context of cyber warfare.

The attribution of a cyber attack is widely considered a fundamental aspect to be resolved before the formulation of every cyber strategy by nation-states. Digital forensics procedures and protocols established in civilian contexts can be adopted by military and intelligence bodies.

The paper explores the field of digital forensics as applied to cyber warfare, mainly for defensive and intelligence operations. It proposed a taxonomy for digital forensics activities and on the time dimension how it is applied to the phases of forensic operations: prioritization, collection, acquisition, analysis, interpretation, reporting/dissemination, detailing a model that tailors techniques to military context, giving also a review of existing literature. Defensive and intelligence activities also need knowledge of the range of anti-forensics techniques applied by counterparts, so an analysis of the anti-forensics arsenal and how it correlates with forensics processes is conducted.

In the conclusion the paper shows the cardinal role of digital forensics (post-attack and in readiness processed) even in military activities and the value of concepts developed in the civilian world, albeit adapted.

## Keywords

Cyber Warfare, Digital Forensics

## 1. Introduction

Digital forensic has come a long way since its inception and has taken by now its place among the forensic sciences. Digital forensic techniques have now reached the state where they are less of an art and more like repeatable and well-documented

scientific procedures. Work-flow phases have been codified in several guidelines developed by practitioners and also in developing international standards like ISO/IEC 27037, published probably 2012.

This paper proposes a model under which digital forensics concepts developed along the years in a civilian context can be usefully applied to military operations, and particularly to cyber warfare. Scenarios in which digital forensics can be useful, and even necessary, include the attribution problem (of cyber attacks), treaty assurance, intelligence and counter-intelligence, both at tactical and strategic levels in the organization.

At first sight the object of digital forensics in a warfare situation is very different from what is needed in the civilian world: here the "final product" is sound evidence, to be used in a court of law -civil or criminal- or at least that can be used, in principle. From there the need to assure the integrity of evidence from the very beginning and along all the chain of custody. In military contexts this necessity may seem unnecessary, compared to the need for actionable intelligence, often within strict time constraints, but contemporary warfare presents us with more and more legal concerns than the past. Contemporary international relations are more and more mad of supranational bodies with varying degrees of legal clout and status, from the United Nations to the International Court of Justice, various regional bodies and alliances, and a long history of international conventions currently in force. More and more we are faced with the phenomenon of nation-states presenting evidence of enemy conduct in order to justify a military action. If cyber warfare is to be a proper part of warfare, these evidence inevitably is and will be in digital form. Another example of digital forensics relevance is the problem of verification of possible future treaties regarding cyber warfare: this a thorny problem, and a very open one, currently debated by legal experts, military bodies and forensic analysts worldwide. It is quite easy to detect ICBM silos, not so easy to detect cyber weapons ready for action. International relations experts and country leaders are faced by the challenge of adapting concepts formulated long ago like aggression of a nation-state onto another, or combatant status, to the realities of cyber warfare. Also the relevance of non-national actors is very high in cyber warfare, by its very nature, complicating again the picture; we have only to think of the proxy problem, where non-national organizations or even individuals can conduct cyber activities on behalf of governments (knowingly or not).

Legal concerns are mentioned because forensics is where the technical side meets the legal one: digital evidence is a tool in a legal process so it is to be conducted keeping in mind legal concerns like jurisdiction, lawful acquisition, and so on.

The rest of this paper will present a brief overview of the field of digital forensics, as we see it now, followed by a short modelization of cyber warfare activities and context. After that a model matching digital forensics to the cyber warfare context will be proposed.

## 2. Digital Forensics

What is digital forensics? We report here one of the most useful definitions of digital forensics formulated. It was developed during the first Digital Forensics Research Workshop (DFRWS) in 2001 and it is still very much relevant today:

Digital Forensics is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.(Pearson 2001)

This formulation stresses first and foremost the scientific nature of digital forensics methods, in a point in time when it was transitioning from being a "craft" to an established field and rightful part of the forensic sciences. At that point digital forensics was also transitioning from being mainly practised in separated environments such as law enforcement bodies and enterprise system administrators to a unified field. Today this process is very advanced and it can be said that digital forensics principles, procedures and methods are shared by a large part of its practitioners, coming from different backgrounds (criminal prosecution, defence consultants, corporate investigators and compliance officers). Applying scientifically derived methods implies important concepts and principles to be respected when dealing with digital evidence. Among others we can cite:

1. Previous validation of tools and procedures. Tools and procedures should be validated by experiment prior to their application on actual evidence.
2. Reliability. Processes should yield consistent results and tools should present consistent behaviour over time.
3. Repeatability. Processes should generate the same results when applied to the same test environment.
4. Documentation. Forensic activities should be well-documented, from the inception to the end of evidence life-cycle. On one hand strict chain-of-custody procedures should be enforced to assure evidence integrity and and the other hand complete documentation of every activity is necessary to ensure repeatability by other analysts.
5. Preservation of evidence – Digital evidence is easily altered and its integrity must be preserved at all times, from the very first stages of operations, to avoid spoliation and degradation. Both technical (e.g. hashing) and organizational (e.g. clear accountability for operators) measures are to be taken.

The definition above goes on listing the work phases that make up digital forensic processes. A slight different sequence is preferred today and is also endorsed by the ISO/IEC guidelines in development:

1. Identification. This process includes the search, recognition and documentation of the physical devices on the scene potentially containing digital evidence.(ISO 2012)

2. Collection - Devices identified in the previous phase can be collected and transferred to an analysis facility or acquired (next step) on site.
3. Acquisition - This process involves producing an image of a source of potential evidence, ideally identical to the original.
4. Preservation - Evidence integrity, both physical and logical, must be ensured at all times.
5. Analysis – Interpretation of the data from the evidence acquired. It usually depends on the context, the aims or the focus of the investigation and can range from malware analysis to image forensics, database forensics, and a lot more of application-specifics areas. On a higher level analysis could include content analysis via for instance forensics linguistics or sentiment analysis techniques.
6. Reporting - Communication and/or dissemination of the results of the digital investigation to the parties concerned.

It is very important to underscore a trend in digital forensics practice, where we are moving away from the classical work flow outlined above and readily applicable for instance to post-mortem processing of hard-drives and other media, to live forensics, where absolute preservation of the media integrity (bit by bit) is impossible or very difficult. This is the result of many developments, some of which are:

- Widespread diffusion of cell phones and other devices which it is very often impossible to access without altering their state;
- Ever more need for network forensics, where live collection and traffic analysis pose some challenges, both technical and legal;
- Very large data: until recently prioritization was not a concern in digital forensics and guidelines recommended that all evidence found was to be preserved, acquired and analysed in depth. Recent recommendations introduced forensic "triage", or prioritization of evidence, which means selecting evidence to be analysed or even acquired, early in the process (during the identification step), reducing work load but renouncing to strict preservation of all evidence. Triage is especially important in military settings, and more so in a tactical setting, where the need for actionable intelligence outweighs other considerations, and a balance between forensic rigour and speed is needed.

In these cases, where some alteration of the evidence is unavoidable, the need for stringent documentation and justification of the process is even more important.

Lastly the definition given above details the objectives of digital forensics, that is the reconstruction of events past but also the prevention of "unauthorized actions […] disruptive to planned operations". The language itself seems to adapt very well to what forensics can do in military context, particularly in intelligence, where the focus is on the future rather than the past.

## 3. Cyber warfare activities and scenarios

Cyber warfare is by now a term widely known to the general public, even a buzzword: its study surely suffers from excessive hype, but -more importantly- also from a lack of clear and broadly accepted definitions. Broad definitions in use for instance include all activities making use of the electromagnetic spectrum, including in this way what is known as electronic warfare and even electronic intelligence (ELINT). For the purposes of this paper a more narrow -and maybe more simplistic- definition is used: cyber warfare comprises military activities -defensive or offensive- involving information networks, and the Internet in particular, including intelligence and counter-intelligence.

The above formulation eschews the word "cyberspace" or "cyberdomain", themselves the object of an ongoing debate: cyberspace is widely recognized as a fifth domain of operations, to be added to the traditional four recognized by the military -land, sea, air and space- but another view is being proposed, negating cyberspace autonomy as a domain of war but considering cyber more of a "subdomain"(Grunert 2011) subtending and informing all the others.

This paper does not adopt a formal definition while proposing to systematize forensic activities in cyber warfare.

### 3.1. Cyber warfare offensive

Recognizing that cyber warfare scenarios are very "liquid", magmatic, and activities with different targets can and are conducted simultaneously, a loose classification is proposed where warfare in the cyber domain can be waged for exploitation, disruption or information warfare.

1. Exploitation: these are activities directed to targets in cyberspace and aimed at acquiring data and information, mostly without damaging the target systems. This is usually achieved by gaining access to networks or single systems. Cyber espionage can be included here, being its object to acquire information, be it direct military intelligence or economic intelligence.
2. Disruption: activities of this kind are aimed at damaging information systems, limiting in one way or another their capabilities. Attacks in this area can range from simple DOS/DDOS (Denial of Service) attacks to targeted penetration of the target systems. In the case of the so-called "*cyberphysical*" systems like industrial networks, disruption activities can cause damage to physical assets and not only information systems.
3. Information warfare: in a military context psychological operations (PSYOPS) have always existed but modern information networks and the cyberspace gave propaganda a wholly new playground. Influence can be

achieved in modern connected societies via operations on the Internet, for instance on the social networks, blogs, media sites.

4. Cyberphysical attacks: when systems like industrial automation networks or infrastructure control systems are targeted, disruption activities can cause damage to physical assets and not only information systems. In this classification this kind of attack is kept separate from disruptions to systems that remain confined to cyberspace. The Stuxnet worm has brought to a wide audience the potential of cyber weapons in this field.

### 3.2. Megatrends and their consequences

Convergence on standard digital technologies in a trend going on for some time and it is likely it will go on in the future, for economic and technical reasons. Industrial automation systems for instance historically implemented networking with proprietary protocols, but the current trend is to use standard protocols born in the IT world, like Ethernet -albeit a dedicated version of it. Also the military is using a surprisingly number of off-the-shelf standard technologies, from operating systems to application software to networking. This, and the growing interconnections of both infrastructure and military systems, obviously facilitates attackers.

The future will bring even more interconnections and pervasive networks with the progressive introduction of IPv6 protocol and its expanded address space: even more nodes will be connected in the so-called "Internet of things". So-called Netcentric Warfare in its different doctrinal flavours is the military manifestation of this trend.

The result is a greater vulnerability of control and weapon systems: we already witnessed attacks on UAV software by malware that could be used to infect a normal office workstation and - in the infowar arena - web defacements and site penetrations. Again Stuxnet comes to mind when we analyse its attack vector on the host PC by exploiting vulnerabilities of commercial operating systems.

### 3.3. Cyber warfare context

Cyber warfare should be framed in its proper context as primarily a form of warfare. Warfare itself has undergone in the last decades a profound evolution: the classical concept of a formally declared war between nation-states does not apply to what is called "war" in contemporary times. New actors wage war, new legal frameworks and fluid scenarios has come into play. Wars sanctioned by international organizations, non-wars where armies are involved like stabilization and peacekeeping operations, wars declared by terrorists networks are instances of contemporary warfare. Cyber warfare - if it is to be called that - have to be inscribed in this context, differentiating itself from cyber crime or individual actions, be they politically motivated or not. Boundaries between what is warfare and what is not and between what actors are involved and what are not are muddled: we propose the following classification for actors in the cyber warfare arena:

1. Nation-states. Included in this category we include military and non-military agencies belonging to sovereign nations. An example of military cyber unit is USCYBERCOM, but cyber activities can be conducted also by "conventional" units, especially at the tactical level. Under this header we consider also national intelligence agencies engaging in information warfare, espionage and counter-espionage. The goal of the nation-states in cyber warfare are the classical aims of gaining military, but ultimately economic and political, advantage;
2. Supranational entities. Military alliances like NATO or *sui generis* confederations like the EU have their structures, agencies, objectives and agendas that not always coincide with their members';
3. Non-national political actors. These have gained importance in the last decade: the most notable example are transnational terrorist networks, to which some attributes of sovereignty are *de facto* attributed, like the capacity of being part – or subject – of an armed conflict. On another plane entirely, NGOs are gaining recognition as independent actors;
4. Politically motivated organizations - like Anonymous – or individuals. Here can be included informal networks like those that animated the Arab springs of 2011. This category is for sure controversial because such groups are at the boundary between political action and actual (civil) warfare.

Not included here are individual cyber criminals and transnational criminal groups, mainly because of their different objectives, in their case economical profit. There are however zones of intersection with the above actors, many of whose engage in criminal activities in order to finance their activities. As an aside we should consider the use of "insiders" by the actors engaged in cyber warfare: they can be recruited by any of the previous groups, so they do not constitute a separate group.

### 3.4. The attribution problem

The complexity of the cyber warfare landscape shown above shows clearly one of the main cruxes of any strategy for this field, i.e. how to identify sources of cyber attacks. These are by nature easier to mask than other types of warfare attacks, also by using proxies. The attribution problem and the proxy problem that complicates it - discern plausible deniability from genuine autonomy of the attacking entity from for instance its parent state is the field of choice of forensics in cyber warfare.

## 4. Matching digital forensics to the cyber warfare context

The principles and procedures of Digital Forensics, starting from the awareness and preparedness procedures are being incorporated in the management of networks subject to the risk of a cyber warfare attack. This is currently more for military

systems, less so for civilian assets like critical infrastructure networks. They are essential because they allow to gather sound evidence of attacks or attempted attacks while restoring functionality of the systems. The use of the evidence collected can range from internal attribution to the actual presentation in an international court of law or supranational organization like the U.N. Security Council. We concern here only on the technical level, i.e. which forensics techniques can be usefully applied.

### 4.1. Computer forensics

Computer forensics have long constituted the mainstay of digital forensics, to the point of being identified with it until recently. It concerns itself with the analysis of single systems, and we include here the analysis of volatile memory (RAM) and storage media. Volatile memory analysis could reveal some of the means, used by attackers, especially the footprint of the software vector if not part or all of the code still resident. Together with media analysis, computer forensics could yeld a detailed timeline of activities on the compromised system, vulnerabilities exploited and also traces of the software used which can form the base for deeper software analysis.

### 4.2. Network forensics

Probably the most important forensic field in a warfare context, obviously because the vast majority of attacks use networks, whether public or private as a vector. It is also one of the most problematic, where the deployment of preparedness procedure is paramount. Traffic on the network to be defended should be collected on a regular basis to be able, in the aftermath of an attack, to have data to be analysed, considering also the trend for attacks and malware persistent in time. Obviously there is a trade-off with storage space and costs, so continuous analysis should be conducted. After an attack forensic analysis of network evidence can be conducted, trying to reconstruct its means. Protocol dissector are a very useful tool in this regard, and the analysis should be conducted at the various level of the protocol pile, from the application layer down to the data link, considering the various encapsulation implications.

### 4.3. Mobile forensics

The analysis of cellular terminals and networks is prominent and it is a subfield of digital forensics that can transcends the purely “cyber” real to be relevant also against “kinetic” actions, for instance when cell phones are used as IED detonators. Mobile forensics evidence sources comprise the single phone (internal memory and (U)SIMS), the cell towers and the network servers. Especially in the last case, cooperation of the mobile operator is clearly needed. Proprietary operating systems and physical interfaces, together with strong security on the SIM card can be hurdles in the evidence acquisition of a phone, even if the diffusion of sophisticated “smart” phones and standardized connectors are easing off this problem. Acquisition of a phone can be basically “logical” or “physical”, where only the second yelds all the content of memory chips: this is often difficult to do because without altering in some way the evidence. Because often mobile phones are strictly connected to a person, all evidence connected with that person's activities and relations are very important, so in addition of the kinds of evidence that can be found on a computer – which most modern phones or tablets are anyway – data on the user's connections – address books, text traffic, emails etc – can help reconstruct his or her network of relations (the real social network).

### 4.4. Embedded systems forensics

The analysis of embedded systems is another emergent subfield in digital forensics, comprising for instance evidence acquiring from Industrial Control Systems like PLCs (Programmable Logic Controllers). This control systems are widely used in industrial automation and, to the point, in many critical plants and infrastructures that are at risk of a cyber attack. Limited capabilities of these devices limit some preventive strategies like file integrity check: trusted copies of the software uploaded should be kept off-line to be checked against the live ones in case of suspected attacks. Like in mobile phones, physical imaging of internal memory is rarely possible, while analysis of commonly used memory cards can be conducted as conventional media acquisition. Analysis of the software however can only be conducted in most cases replicating the proprietary environment in which it was developed.

### 4.5. Malware analysis

The "raw material" for this analysis can be supplied by any of the above activities, and it is usually one or more executable files or binary libraries. Reverse engineering allows the analysts to reconstruct the behaviour and in some cases most of the source code of the malware. Modus operandi of the weapon and sometimes small pieces of evidence embedded in the code can be pieces of the puzzle of the attribution.

## 5. Conclusion

Digital forensics as a field brings a lot to the arsenal of states and organizations engaged in cyber warfare defence. Its principles and technical procedures, while not decisive in themselves, can help in tackling the attribution problem, one of the thorny dilemmas in cyber warfare. From there, integration of forensics at the policy level should be pursued and recommended.

**References**


Grunert, F. (2011), "*Cyberwar- Probleme für die internationale Politik*", Universität Osnabrück.

ISO/IEC (2012), "*ISO/IEC 27037: Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence*".

Pearson, G. (2001), "*A Road Map for Digital Forensic Research*". Report from DFRWS 2001, First Digital Forensic Research Workshop, Utica, NY.