Chapter 14
Attribution

Clement Guitton
King's College London, UK

ABSTRACT

Attribution, finding the identity of actors behind an attack, is of primary importance to be able to classify an attack as a criminal act, an act of war, or an act of terrorism. But attribution is difficult. Many experts and analysts have explained this difficulty with technical arguments. This chapter seeks to bring nuances to such arguments closely analysing how attribution functions. It brings a focus on political factors constraining attribution, and on specifically three ones: standards of evidence, time, and private companies. It makes three main arguments. Firstly, standards of evidence are only secondary to the political will to attribute an attack. Secondly, time cannot only be reduced; the context surrounding attribution is as much important. Thirdly, companies' important role in attribution also gives ground for accused party to easily undermine their claims. The chapter concludes with opening up the debate on the usefulness of meta-data for attribution.

INTRODUCTION

Attribution, the process of finding out the chain of actors involved in a cyber attacks is important for three distinct reasons. The first one is rather technical, and concerns the model of thinking about security in terms of a 'parameter' to defend (Gady, 2010). To defend information systems against cyber attacks, the model advises to integrate technical solutions such as firewalls or intrusion detection systems. Such techniques were particularly well suited against the mass outbreak of viruses that propagated in the years 2000s, but today's attacks look a lot different. They are targeted and the perpetrators are well resourced to develop attacks evading such measures. Hence, the rationale behind attribution is that instead of focusing on technical solutions to thwart the attack, finding the perpetrator of attacks allows the victim to then take a series of measure against the instigators. These series of measures can range from merely shaming the actors, to diplomatic actions, to incapacitating the instigators by jailing them for instance, if they are criminals.

A second argument for focusing on attribution follows directly from the first one. By ensuring that one has the capacity to attribute attacks, it is possible that the capacity will deter other actors from launching

DOI: 10.4018/978-1-5225-7912-0.ch014

similar attacks. Fearful of the consequences attackers could face, and assuming that the attackers follow a strictly rational decision-making thought process, the likeliness that the victim will find them can outweigh the benefits of launching an attack in the first place and deter them from proceeding further. Unfortunately, deterrence is not so straightforward, and the empirical record proving that attribution can be effective in deterring attacks is rather mixed, in a criminal and international relation context (Guitton, 2012). The case of the Mandiant report offers a sharp reminder of this difficulty. Mandiant, a cyber security company, published a report denunciating the Chinese military as instigators of attacks on 141 US companies in February 2013. High officials used the report to confront China on this issue. Following publication, the attacks stopped but only for two months before resuming with the exact same modus operandi (Sanger & Perlroth, 2013).

Lastly, a third argument for focusing on attribution is that it allows the distinction between what types of response is the most appropriate to a cyber attack. If a state is behind a cyber attack, the measures taken are entirely different than if a criminal individual is. Attribution involves making the distinction between different types of actors, and to know which further processes will be engaged as a result of the cyber attack.

Attribution is therefore an important aspect for tackling cyber threats, and needs careful attention from students of cyber security. Unfortunately, attribution is also difficult and raises many different questions. What makes attribution difficult? How do different actors go about achieving attribution? What are the policy and strategic implications of striking an 'appropriate' balance for attribution between being anonymous online and being secure?

A common quick answer to these questions is that attribution is difficult because of the way the Internet is engineered. But this answer is misleading and highly insufficient for anyone looking closely at attribution. This chapter starts, firstly, by delving into the current debate on attribution and shows that much of the current debate approaches the difficulty of carrying out attribution as lying in technical elements. Secondly, the chapter continues with refuting those claims and breaks down the constraints for attribution into three main ones: the standards of evidence, the time required for carrying out the process, and the role of private companies. Thirdly and lastly, the chapter analyses the relevance of meta-data collection by intelligence services and law enforcement agencies for attribution and the far ranging ripple effects that the debate on attribution has on privacy, anonymity and Internet governance.

Background: Current Approach to Attribution

The current debate in academic and policy circles on attribution is heavily technically oriented. It assumes that attribution is technical, and that it requires as such technical solutions. This is only partly correct.

To traceback the origin of an attack, be it from a denial of service attack or from a malware, it seems *a priori* useful to know the genuine IP address from which the attack originates. Attackers can easily forge the IP addresses of the traffic they send, and can also route it via several computers they already control to make the victims believe it originated from a specific location. Both of these aspects make it difficult to trace back traffic to its real origin, and has led prominent figure, such as Mike McConnell, former director of the NSA, to state that 'we need to reengineer the Internet to make attribution more manageable' (McConnell, 2010). Many other policy makers have embraced this view, including the former directors at the FBI Shawn Henry and Steven Chabinsky (Chabinsky, 2013; Kaplan, 2012). Christopher Painter, the State Department Coordinator for Cyber Issues, similarly stated in a briefing: 'One of the