Inside the Enemy's Computer: Identifying Cyber-Attackers, by Clement Guitton, London: Hurst & Company, 2017, pp. 304, £ 17.24

Munish Sharma*

Attribution of cyberattacks is an impending issue in enabling a credible deterrent against both state and non-state actors. It applies equally to cases of a criminal nature as well as to those with implications for national security. The technology underlying cyberspace facilitates anonymity and thus affixing responsibility, that is, attributability, is not merely a technological challenge but a political one as well, especially when nation states have proven prowess in engaging their adversaries in cyberspace. This is the central argument of the book *Inside the Enemy's Computer: Identifying Cyber-Attacks* by Clement Guitton, one of the first exhaustive endeavours in this direction. In the six chapters, the author delves into the political dimension; discusses the mismatch between the domestic and international legal standards; the rising importance of companies in attribution; and, finally, elaborates upon the time factor, plausible deniability on part of the nation states, and a series of issues in attribution.

The author has analysed attribution in the broader contexts of crime and national security as, he argues, cyberattacks are increasingly moving towards being designated as acts of war, crime or terrorism. It is critical to identify the authors of cyberattacks, either to prosecute the

* Munish Sharma is a consultant at the Institute for Defense Studies and Analyses, New Delhi.

ISSN 0976-1004 print

Journal of Defence Studies, Vol. 12, No. 1, January–March 2018, pp. 101–104

individuals for the acts of crime or terrorism or to exercise retaliation through diplomatic, economic or military options in the case of nation states. In the beginning, while setting out the context for the book, the author outlines three misconceptions vis-à-vis attribution which remain the core element throughout. These misconceptions are: (1) attribution is perceived to be a technology problem, (2) it is unsolvable, and (3) it is challenging because cyberspace is a unique domain when compared to other physical domains.

As a critique of the viewpoint that attribution is a technology problem only, the author explores other factors, such as political and legal constraints in cyberattacks, besides the technical constraints. Guitton supports a nuanced approach to attribution, with varying degrees or range of nuances, rather than looking it purely as a problem that is either 'solved' or 'unsolved'. Also, attribution evolves and changes over time as more information and evidence is gathered by different parties involved in attribution, such as cyber security companies, intelligence agencies, law enforcement agencies and even the private individuals.

In a few instances, Guitton uses the theories of international relations to explain concepts. He also invokes the thoughts of Hans Morgenthau to strengthen his point that pursuing attribution reflects the will of the nation state to maintain, increase, or assert its power. Using detailed analysis of examples and cases the author manages to support his arguments throughout the book. He also discusses existing models of attribution, such as the one proposed by Thomas Rid and Ben Buchanan. Setting the political context, the author argues that attribution is not merely the identification of the attackers but the process of unravelling the entire chain of individuals, organisations and states involved in the attacks; and that the decision to do so in the national security framework lies with the executive arm of the government. Political leadership, the intelligence community, and the premier law enforcement agencies are the credible actors whose words and actions matter while attributing a cyberattack.

The author has also raised the question of how to classify cyberattacks as a national security threat, which demands further research as it is practically quite hard to distinguish between different levels of threat—depending upon the target of the attack, the damage incurred, and even the severity of the attack. Again, using the Sony Pictures hacking instance as a discreet case, the author has highlighted how the United States (US) President and the intelligence community was dragged into the conflict

where a private company was the target of the attack and not the critical infrastructure or any government department.

The author further delves into the pertinent issue of affixing responsibility under the circumstances, especially when it is hard to establish the linkages of the perpetrators of the attack with potential sponsors which could be nation states. States also rely on hacking groups and proxies to execute covert operations and plausibly deny their involvement in or sponsorship to the attacks, reducing the risks of escalation. He argues that no technical solution can help establish the connections between the attacker and the mandating state and, therefore, forensic evidence should be analysed in the geopolitical context along with non-technical means of intelligence gathering. He also deems it necessary to pursue attribution in the wider context, with the help of political experts and journalists in addition to technical and intelligence experts. Guitton also underlines a few of the difficulties that impact the credibility of the attribution when it is solely led or dealt by intelligence agencies. The evidence in such cases is not publicly verifiable owing to its confidential nature. Moreover, it is quite challenging for the political leadership to convince the international community as well as its own citizens of the necessity or rationale for its actions, especially if the state wants to opt for retaliation as part of its deterrence strategy.

A dedicated section of the book highlights the growing importance and influence of companies in the business of cyber security. According to the author, a lot of these private entities such as Mandiant and Kaspersky Lab have rich technical expertise to investigate cyberattacks and the requisite contacts to influence or even shape the diplomatic agenda for bilateral discussions. The example of Mandiant has been discussed in much detail along with the role it has played over the last six to seven years in shaping the bilateral discussions on cyber security between the US and China. Guitton goes on to discuss, although in brief, the budding numbers of specialised companies selling services such as hacking and zero-day vulnerabilities to states, as the practice grows into an unregulated market.

The author also outlines few of the ways for attribution which are prevalent at present: the geopolitical context, the political character of the victim, probable beneficiaries of the attack, apparent origin of the attack, and the sophistication and scale of the attack. Towards the end of the book, Guitton gives substantial examples and analyses to conclude that attribution should be dealt as a process, and not a problem. It is a

time-consuming process, quite similar to the real-world investigations of crime. Also, the private companies are increasingly playing an important role in this arena, with their proven prowess in technology and deep contacts within intelligence agencies or the governmental apparatus. Towards the conclusion, Guitton brings out a very important point pertaining to the use of attribution in the political calculus. According to him, the standard of the evidence is flexible and it depends on the wider political and economic relations of the victim state vis-à-vis the probable or apparent instigators. The victim state has to evaluate the political gains out of the exercise or process of attributing. Timing, in this case, is of utmost essence to use attribution for important political leverage. However, the will to act is important, rather than the evidence, the author concludes.

The book is an outcome of thorough research work and reflects the experience of the author as an analyst with the Swiss Department of Defence. Rather than merely touching upon the technical aspects of attribution the book takes a deep dive into the spectrum of other factors which influence the outcomes of the process of attribution. Extending the purview of attribution beyond the handful of actors, the author has made significant contribution to the literature on this subject, and more research on this aspect would unfold in interactions of policy, technology and judicial aspects on the subject. The extent to which examples and policy statements from the political leadership and technical experts have been used to support the argument and these add considerable value to the research work.