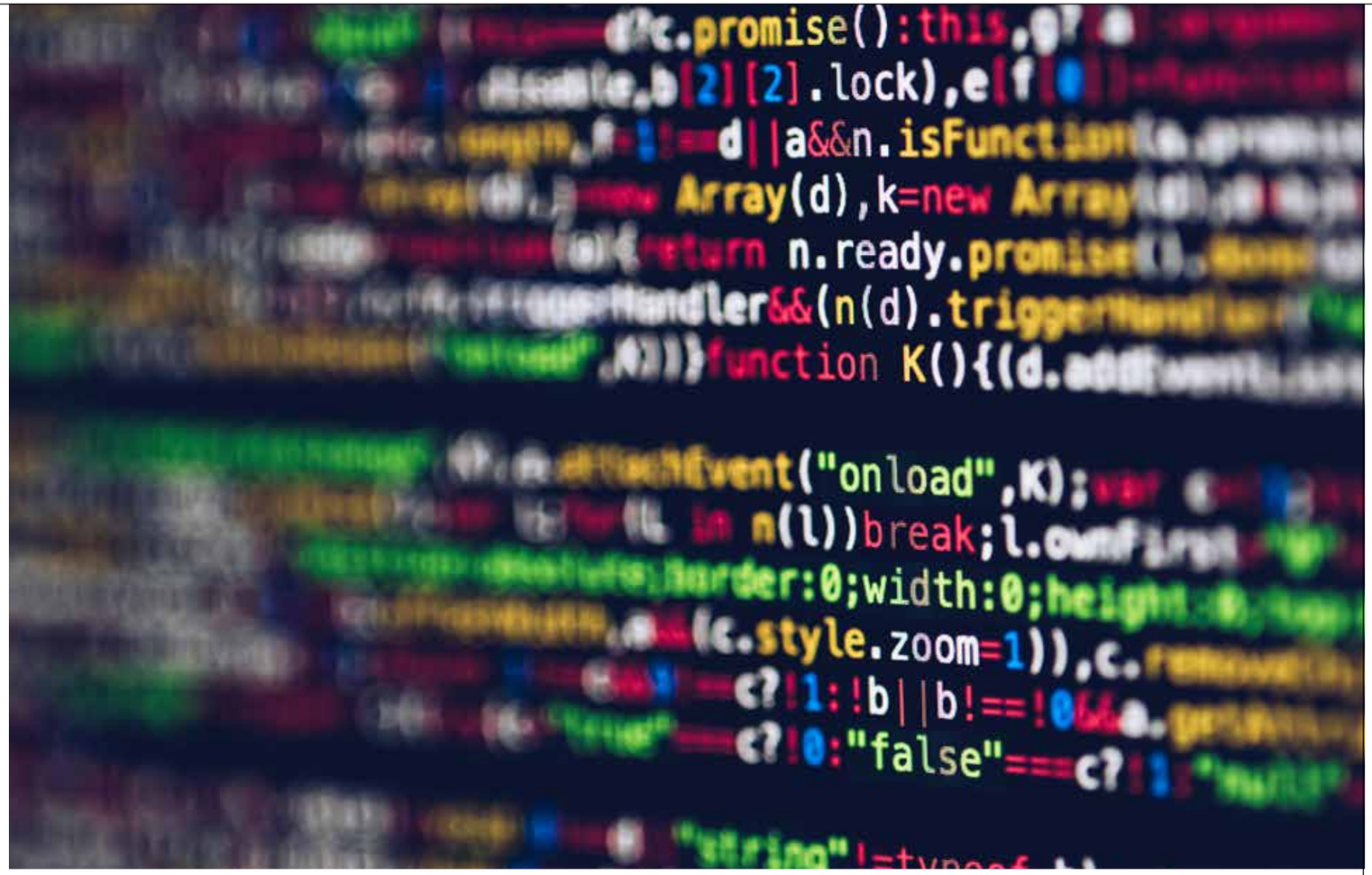
MASTERING DATA

Alain Vernadat *examines the need to put data at the heart of the investigation*



Data explosion is a reality, and it has become the golden nugget of the 21st century. As the volume of digital data generated per year is growing exponentially, this new dimension is shaking up the way in which law enforcement agencies and investigation services operate. The world of digital evidence is rich and complex in equal measure. A whole variety of data and metadata actually circulate at the core of every investigation: text, audio, video… Despite their critical nature, accessing and preserving such data and metadata is still a complicated business, and many hurdles exist, as well as the challenges raised by such a major transformation.

An expert in investigation technologies and services for global security, Deveryware has recently published its white paper, *Data At The Heart Of The Investigation*, on this major issue. As Jacques Salognon, the founding President of Deveryware, explained: "it is an exciting, but complex subject, and it involves significant challenges – for the advancements brought about by data prefigure the contours of tomorrow's investigations." With this white paper, Deveryware ambitions to foster joint reflection, to address the questions market players and all relevant stakeholders have regarding the issue of security. It also illustrates the approach supported by the group – one built on innovation, growth and a forward-looking vision.

IT IS OUR DUTY TO TRY TO INNOVATE AND PROVIDE SECURITY SOLUTIONS THAT REMAIN ETHICAL

The white paper constitutes a dive into data. It addresses all the issues relating to this major evolution and questions leading figures from the industries of security and new technologies, and from the legal sphere, and also provides answers to such topical issues as: what challenges will intelligence and investigation stakeholders have to face in handling such data? What hopes do those new smart analytical tools represent in the fight against organised crime, terrorism, cybercrime, financial fraud, etc.? What are the challenges that need to be addressed technically, legally, culturally and politically, at the national and European levels? How can we prepare for the future and fight upcoming threats within an ethical and accountable framework?

Data is becoming critical within digital investigations – but encouraging its preservation and preventing its alteration and falsification involves many challenges. It has therefore become urgently necessary to support the state services in processing and analysing this data and metadata more efficiently, while understanding the specificities and weaknesses of digital evidence. In parallel to that, it's essential for investigators to be able to enhance their mastery of the methodology.

Investigation technologies need to adapt as our digital world is subject to ever-growing threats (network breach, data leaks, insider threats, malwares, ransomwares, bitcoin scams for organised crime, terrorism, fraud, economic and financial fraud, cybersecurity) – threats that evolve as do new technologies: the Cloud, AI, IoT, 5G, etc. In the era of Big data, the key players in the fields of intelligence and investigation need to have high-performance, intelligent analytical tools.

As Guillaume Kauffmann, Managing Director of Tracip, explains: "It has become difficult for an investigator to summarise large amounts of information quickly and effectively. As for the analytical tools, they are capable of processing and exploiting large amounts of data and information flows almost in real time." Analytical platforms actually do provide a suitable solution to such a challenge: processing and exploiting large amounts of data and information flows almost in real time. These analytical tools represent untapped potential in addressing threats: time saving for investigators, new avenues being explored, decision support, the decompartmentalisation and sharing of information.

Supporting innovation and the digital revolution must also lead to introducing more agility so as to strengthen the capacity for foresight and analysis, as well as increasing our operational agility, with humans continuing to be the central pillar at the heart of these developments. "All the things that our experts are developing only have meaning in terms of supplementing the intuition of the investigator or officer. We put human intelligence back in where it is most useful, ie in the interpretation. The tools are thus very much focused on the end user," adds Xavier Houillon, Assistant Director of OAK Branch.

The evolution of technologies associated with mega-data and artificial intelligence is enabling us to envisage going far further in terms of using the data for the struggle against criminality and delinquency in all their various forms. Time savings for investigators, new avenues being explored, decision support, the decompartmentalisation and sharing of information… these collaborative and smart interoperable platforms make it possible to extract and capitalise on the value that this data represents in the interests of truth or the anticipating of criminal phenomena, in order to work towards creating a safer world. Deployments with Interpol, Germany and Belgium, in particular, show the extent to which analytical platforms like this can be of great interest and usefulness to operatives handling sensitive files.

Investigation technologies need to adapt as our digital world is subject to ever-growing threats

Over and above what is inherently interesting about these platforms, the success of such projects is founded on strengthening cooperation between state actors, industry stakeholders and European and international actors, who must be able to evolve within technical, regulatory, ethical and financial frameworks that are transparent and coherent. Operational experience shows that many threats and attacks are planned and organised from outside Europe. It is therefore necessary to have greater collaboration at European and international level.

Pursuing criminals across borders means pursuing cooperation with Europol, Eurojust or indeed Interpol, and reinforcing a more efficient means of sharing information thanks to interoperable tools and a harmonised legal framework within Europe, but also at the international level. While the European Investigation Order is a big step forward, E-evidence must make it possible to go further.

Those challenges also encompass the issue of technological sovereignty between France and Europe. Promoting cooperation between the public and private sectors as well as building a joint strategic vision, constitute a solution to address the challenges, if we do not want our information and investigation services to be deprived of a great opportunity and to be lagging behind their partner states.

Supporting innovation and the digital revolution must also lead to further taking down of the barriers between worlds, while striving for greater agility so as to strengthen the capacity for foresight and analysis, nourish strategic and doctrinal thinking and increase our operational agility.

There is a pressing need to devise a funding and investment model to support the development of a French and European industry of homeland security and Big data. The public procurement regarding French and European excellence is one of them. Just as the automobile and aeronautics sectors have been supported by the state – notably to prevent our

industry from lagging behind China or the United States, so should industries from the security sector. It should become a national and European priority in a hyperconnected and interdependent world.

Companies nowadays have the responsibility to foster trust in order to increase the safety of digital processes, products and services. Many private actors already work together on the measures that should be taken towards building a French model for ethical data management. For these tools must indeed serve the general interest, with a need to develop smart and collaborative platforms that comply by the regulations in force in France and Europe, while being embedded within an ethical and accountable approach. It is our duty to constantly reflect upon the ways in which we can innovate and provide security solutions that remain ethical.

THE FIGHT AGAINST CRIME, FRAUD AND TERRORISM IS INCREASINGLY TAKING PLACE IN CYBERSPACE

Multi-dimensional threats, an unstable and unpredictable strategic context, an increasingly complex and interconnected world – such is the environment in which the security forces are working towards ensuring global security. The threat of terrorism is a lasting one and is currently entering the field of digital and social networks on a huge scale. Financial criminality remains a complex phenomenon, one that is growing and costly, and the COVID-19 pandemic and its expected economic consequences are likely to exacerbate this threat and create new vulnerabilities. The production of counterfeit goods is a troubling global phenomenon and the threats linked to digital vacillate between increasing sophistication and opportunism. The fight against crime, trafficking, fraud and terrorism is nowadays increasingly taking place in cyberspace – and the threats there are quite real.

GROWING THREAT

Cybercrime is expanding its sphere of activity with each passing year. As new technologies and new uses come into being, so the space that could potentially come under attack constantly increases. Ransomware, spear-phishing, crypto-jacking, skimming, and sextortion are now the kinds of things investigators deal with on a daily basis. The damage done by cybercrime is estimated to cost almost $6,000-billion a year.

It is therefore time to react and prepare the future of investigation: opening up the new chapter of predictive capabilities, so as to foresee and anticipate the criminal acts of tomorrow. Tools are useful and essential in our hyper-connected society, but they must be developed and used to serve the general interest.

We have the power to bring about a safer world, by mastering data and the ways in which it is processed, by cultivating a spirit of information sharing and cooperation within a harmonised legal framework, to which the power of these supporting technologies will bring a whole new dimension, and make security a close ally of liberty. All that will only be possible, however, if we commit, together, to ethical developments and relationships of trust. The shared objective of tomorrow's world thus seems to emerge as a desire to strive for a safer world through innovation, commitment and ethics ●

Alain Vernadat has been Managing Director of the Deveryware Group since 2013 and is in charge of defining and executing the company's strategic roadmap. He manages and coordinates all operational teams: design, R&D, sales, operations and support.

The threat of terrorism is entering the field of digital and social networks on an unprecedented scale