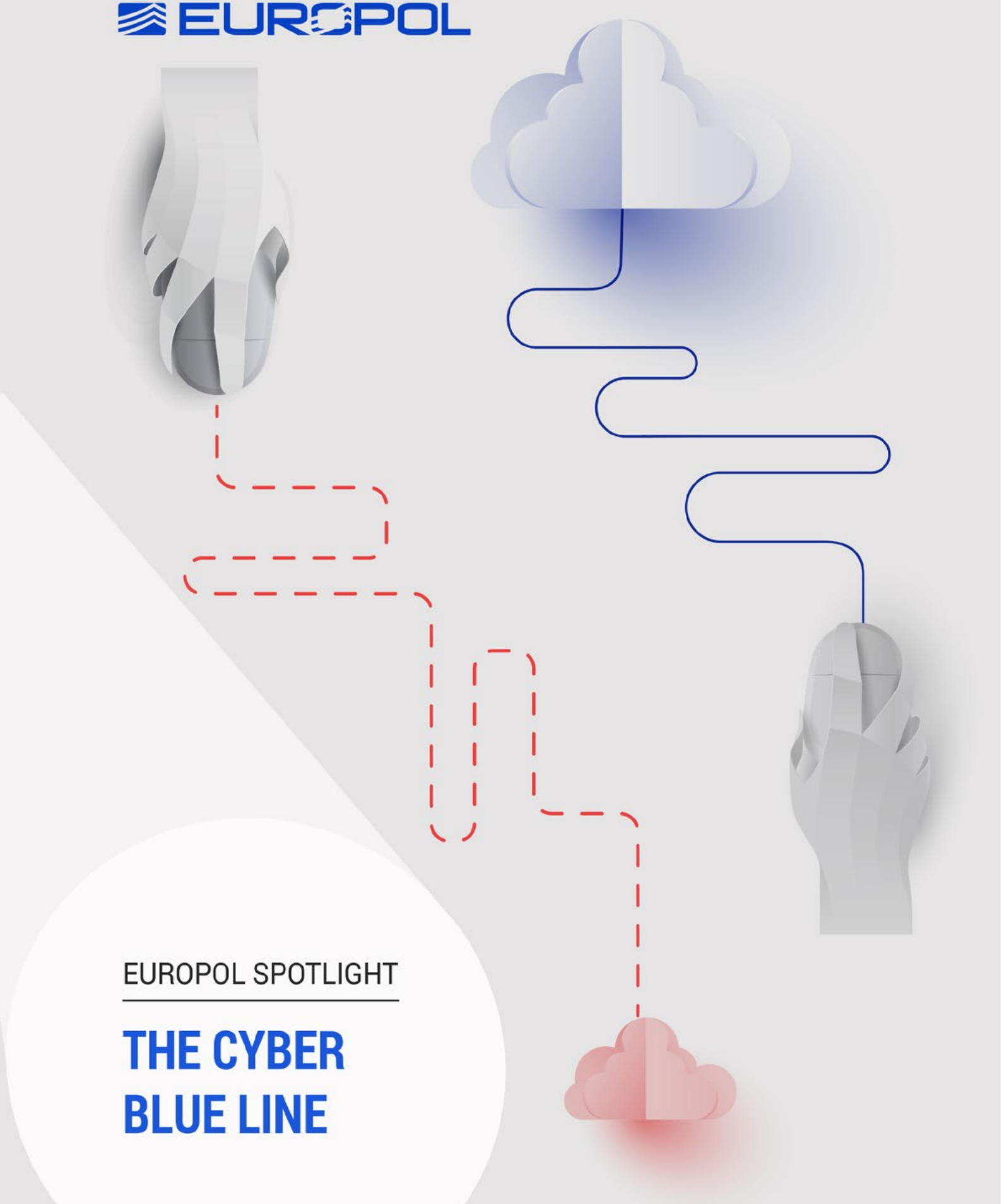
EUROPOL



EUROPOL SPOTLIGHT

THE CYBER BLUE LINE

FOREWORD

As technology evolves, so does our society and with it the role of law enforcement. A significant and increasing aspect of law enforcement work is now dedicated to providing safety and security online. This not only means protecting the rule of law and victims online, but also serving the online community. In doing so, law enforcement is confronted with a number of challenges that, at their core, link to the question on where to draw the line.

Cyberspace is a new, borderless and constantly expanding societal domain, which increasingly blurs the line between the real and the online world. The evolving environment of cyberspace opens up incredible opportunities for our digitised societies as outlined in the European Commission's vision for a successful digital transformation of Europe.

Unfortunately, it can also create opportunities for criminals, and poses an ever increasing risk to safety and security online. As our lives continue to move online, so do criminals, aided and abetted by a booming cybercrime economy, which equips them with the means, method and opportunity to commit cybercrime. As we highlighted in our recently published SOCTA 2021, this contributes to a 'criminal hydra' where even successful and far-reaching disruptions of criminal networks have little or no long-term impact in terms of supressing the activities of organised crime, thereby not only undermining Europe's economy and society but importantly weakening the rule of law. Technology and more specifically the criminal abuse of technology plays an essential role in this regard.

Traditionally, we as law enforcement have been early adopters of technology and have consistently adapted to new technologies, particularly in relation to tackling criminal abuse. Equally, our role in cyberspace emphasises the relevance of existing concepts such as community policing and its potential to manifest online.

This position paper by Professor Mary Aiken, Professor of Forensic Cyberpsychology at the University of East London and an Adjunct Professor at University College Dublin, Ireland; and Dr Philipp Amann Head of Expertise & Stakeholder Management, European Cybercrime Centre at Europol highlights these changes, summarises the main challenges and identifies a number of pertinent questions that require both thought and cyber leadership, and can perhaps help to inspire and inform necessary multi-stakeholder dialogue - we are all in cyberspace together.

Europol as the collective voice of EU law enforcement and charged with upholding the core principles of serving and protecting the population, can play a pivotal role in helping shape the future of law enforcement, in the real-world and in cyberspace. This can be achieved by providing a platform for essential discussions and by facilitating necessary multi-stakeholder dialogue to discuss responsibility, accountability, safety and security now mediated by technology.

And in doing so, collectively decide where to draw the Cyber Blue Line.

Catherine de Bolle

EXECUTIVE DIRECTOR OF EUROPOL

The 1854 Battle of Balaclava is best known for the disastrous Charge of the Light Brigade, a failed military action led by Lord Cardigan against Russian forces. It is less well known for the *'Thin Red Line'* incident, whereby the distinctively red uniformed Scottish Highland regiment formed a long line and somewhat extraordinarily managed to halt a Russian cavalry charge**.** The phrase is still in use today and is often used to describe a "thinly-stretched group resisting greater forces, including, as the *'Thin Blue Line*,' the police."[1]

The 'thin blue line' started as a phrase and has been around for some time; it was reportedly first used in 1922 by New York police commissioner Richard Enright[2] and then became popularised as a graphic image, a blue line flag. It is seen on everything from police cars to coffee cups and COVID-19 masks. Only recently has the thin blue line flag sparked controversy.[3] No doubt, officers may wear blue line flag imagery with a sense of 'protect and serve' pride. However, some view this linear symbolism as unhelpful when it comes to community-police relations. Last year it was reported that San Francisco's police chief asked his officers to wear neutral face coverings as he was concerned that some might perceive the symbol as "divisive,"[4] more recently, as rioters breached the Capitol, some were photographed waving pro-police thin blue line flags.[5]

Domain of Operations

In 2016, another significant event took place when NATO ratified cyberspace as a domain of operations, acknowledging that future battles would take place on land, sea, air, and computer networks.[6] There are also efforts at the state-level to mitigate the risk of cyberspace activities impacting the so-called 'real-world.'[7] We have long debated the role of policing in real-world contexts, in terms of authority, power and persuasion. However, the nature of civil society is evolving in tandem with technological developments reflective of nuanced changes within communities and respective societal values, along with considerations

1 https://www.nms.ac.uk/explore-our-collections/stories/scottish-history-and-archaeology/the-thin-red-line/
2 https://www.politico.com/news/magazine/2020/06/09/the-short-fraught-history-of-the-thin-blue-line-american-flag-309767
3 https://www.police1.com/police-history/articles/what-does-the-thin-blue-line-flag-mean-2J3500lyyaGueEo0/
4 https://apnews.com/article/e6757f9761d5302a2fdb5712fa915c5e
5 https://www.washingtonpost.com/local/capitol-police-officers-support/2021/01/08/a16e07a2-51da-11eb-83e3-322644d82356_story.html
6 https://www.nato.int/cps/en/natohq/topics_78170.htm
7 https://www.osce.org/cio/288086

regarding privacy, protection of personal data, fundamental rights and perception of security. The threat landscape has also evolved, attribution is complex in cyber contexts, cybercrime is growing in scope, number of attacks, financial impact and sophistication, jurisdiction is problematic, and the range of offenders and threat actors continue to grow[8]. The cavalry charge of the Battle of Balaclava is now taking place in cyberspace, at the speed of solar wind, with state-sponsored or condoned threats often leading the attack, along with organised cybercrime gangs, and hacktivists. Somewhat concerningly, all displaying increasing levels of convergence.[9]

As highlighted in Europol's recently published Serious and Organised Crime Threat Assessment, SOCTA 2021, this contributes to a 'criminal hydra'[10] where even successful and far-reaching disruptions of criminal networks appear to have little or no long-term impact in terms of suppressing the activities of organised crime. This not only undermines Europe's economy and society but, importantly weakens the rule of law.

The Evolution of Policing

The first policing organisation originated in Egypt some five thousand years ago. Since then, with each new challenge in each jurisdiction, the practice of policing has evolved and adapted. Magistrates protected the city-states of ancient Greece, supported at times by Scythian slaves, 'hue and cry' policing in medieval England focused on collective responsibility, keeping the peace for community protection. The first modern and efficient system of policing was established in 17th Century France following a plague and food riots that threatened social order. The UK Thames River Police was also a circumstance led and somewhat reactionary initiative, founded in 1798 to address theft and looting from ships anchored in the port. Interestingly, it was financed by the merchants of the day. The first motorised patrol car used by US law enforcement appeared in the early 1900s, police needed cars to keep up with motorised vehicles driven by offenders, such as the infamous

8 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020, https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime

9 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015
https://www.europol.europa.eu/iocta/2016/convergence.html

10 Hydra - a gigantic mythical monster with multiple heads https://www.britannica.com/topic/Hydra-Greek-mythology

criminals Bonnie and Clyde.[11] Adoption of radio communication systems and full motorisation was accomplished after World War II; the presence of police cars in US city streets was considered to have deterrence value and reassured citizens of their safety.[12] On a European level, the EU's law enforcement agency Europol was established in 1999, an initiative designed to help European law enforcement authorities collaborate to fight serious international crime and terrorism. In 2009 Europol became a full EU Agency when it came under the EU's competence with the Lisbon Treaty. Today, Europol's position is at the heart of the European security architecture, which allows the agency to offer a unique range of services to the international law enforcement community.

Police as Early Adopters of Technology

Police have been early adopters of new concepts and technologies, from the establishment of the United States National Crime Information Center in 1967 to the European Schengen Information System in 1995. International law enforcement organisations such as Europol also maintain sophisticated tools and computerised databases, comprising of DNA records and photographs that assist in the fight against terrorism, drug trafficking, child exploitation and abuse, trafficking in human beings, money laundering and other forms of organised crime. More recent examples of innovation in policing worldwide include Artificial Intelligence-based approaches, the handling of large data sets, along with vehicle and drone forensics.

Advancements in industry have long influenced policing developments, often in response to criminals abusing these advancements to further their illegal efforts. For law enforcement, this has created new opportunities but also led to significant new challenges. The criminal abuse of encryption, an essential element of our digitalised democracies, and other privacy-enhancing technologies and designs[13] have created an imbalance between privacy, security and safety. This is currently impeding criminal investigations and police ability to uphold the rights of victims and criminal justice.

A Constantly Expanding Cyberspace

The world has changed geographically as the line between the real, and the

11 https://www.fbi.gov/history/famous-cases/bonnie-and-clyde
12 https://www.britannica.com/topic/police
13 Examples include DNS over HTTPS, Oblivious DNS over HTTPS, Carrier-grade NAT or 5G

online world continues to blur. Cyberspace is a new, borderless, constantly expanding societal domain, an 'Internet of humans,'[14] from surface web to deep web, and dark web to darknets. New cybercriminality platforms, tools and tactics have created a booming cybercrime economy[15] and lowered the entry-barrier for criminals to commit cybercrime, as they no longer need the technical skills to do so. This is linked to the Crime-as-a-Service (CaaS) business model, which grants easy access to criminal products and services, thereby enabling a broad base of cybercriminals to launch attacks of a scale and scope disproportionate to their technical capability and asymmetric in terms of risks, costs and profits. The severe and significant consequences of this have been evidenced by recent ransomware attacks facilitated by the evolving Ransomware as a Service (RaaS) 'business model'.[16]

The pandemic has further illustrated the agility and adaptability of criminal enterprise, unscrupulously profiting from illicit trade in everything from fake vaccines to counterfeit Personal Protective Equipment (PPE).[17] It has also brought to fore the significant problem of mis- and disinformation online, resulting in real-life action and consequences. Examples include physical attacks against GSM towers inspired by conspiracy theories involving 5G, a cyberattack against the European Medicines Agency and the subsequent leakage of stolen data and communication, which according to public reports, were manipulated to potentially undermine trust in vaccines.[18]

These examples and others emphasise the need to factor in the risks of such activities in cyberspace, spilling over into real life, compounded by societies' increasingly fragmented response.

Cybersecurity and Safety Tech

The economic costs of cybercrime are high, but the social costs are even

14 The internet of humans https://ec.europa.eu/digital-single-market/en/blogposts/internet-humans
15 human and technical drivers of cybercrime https://www.ccdriver-h2020.com/project
16 In May 2021, the Irish Health Service (HSE) was under siege in terms of a "catastrophic" hack of its IT systems. https://www.bbc.com/news/world-europe-57184977. The HSE has secured injunctions from the Irish High Court "restraining any sharing, processing, selling or publishing of data stolen from its computer systems in a massive cyberattack" Notably the orders are against "persons unknown" a highly unusual legal order https://www.irishtimes.com/news/crime-and-law/courts/high-court/hse-secures-injunctions-restraining-sharing-of-hacked-data-1.4570769
17 https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime
18 https://www.ema.europa.eu/en/news/cyberattack-ema-update-5

higher; people are being subjected to cyber scams, to fraud and blackmail; they are being coerced, trafficked, harassed and stalked. The most vulnerable members of society, children and young people, are particularly at risk of sexual exploitation and abuse. Notably, the COVID-19 crisis has resulted in significant increases in activity relating to child sexual abuse and exploitation, which was already at high levels prior to the pandemic.[19]

For decades, the emphasis has been on cybersecurity solutions to online threats. However, cybersecurity primarily focuses on protecting data, processes, networks and systems. It does not focus on protecting what it is to be human, what it is to be a society, and this has perhaps contributed to a protection governance gap. Technological innovations may help to address this problem; a new online safety technology sector coined *'Safety Tech'*[20] is evolving, designated in the UK, and emerging in the US,[21] which seeks to offer technology augmented solutions to technology-facilitated online harms.[22] Safety Tech focuses on protecting people from a range of online harms and crimes, from harassment to child sexual exploitation and terrorist content online.[23] Undoubtedly, online safety technologies will be a productive future resource for policing, particularly when online harms and cybercrime now have 'Big Data' type proprieties; namely, volume, velocity, and variety.

We must become more cognizant of broader societal order issues, such as the increased attack surface created by the lockdown induced hybrid office, the digital pivot to large scale remote working, and concomitant increased human psychological vulnerability precipitated by the pandemic crisis. We need to recognise and then navigate increasing social complexity such as juvenile cyber delinquents engaging in hacking and cybercrime. We need to work towards differentiating technology-facilitated adolescent risk-taking behaviours such as the sending of messages, images and videos of a sexual nature, from serious criminal sex offending, and deploy appropriate interventions. As a society, we will have to address offender convergence dark web settings[24] and rampant cybercriminality facilitated by the premise

19 https://www.europol.europa.eu/sites/default/files/documents/europol_covid_report-cse_jun2020v.3_0.pdf

20 Safety Tech:"Safety Tech providers develop technology or solutions to facilitate safer online experiences, and protect users from harmful content, contact or conduct" Donaldson, S., Davidson, J., & Aiken, M. (2020). *Safer technology, safer users: The UK as a world-leader in Safety Tech*. London: DCMS. p.71

21 Aiken, M and Donaldson, S. (2021) *Towards a Safer Nation: the United States 'Safety Tech' Market*. Paladin.

22 https://www.gov.uk/government/consultations/online-harms-white-paper

23 https://www.gov.uk/government/news/new-report-reveals-uk-as-world-leader-in-online-safety-innovation

24 Felson coined the term 'offender convergence settings' to describe certain physical locations, e.g. local tough bars, in which (potential) offenders meet each other. Here they relax with friends and acquaintances, meet new people, exchange information, sell stolen material or plan new criminal acts. The perpetrators of cybercrime also make use of such locations, albeit digitally in so-called virtual forums" (p.111) Soudijn, M.R.J., Zegers, B.C.H.T. Cybercrime and virtual offender convergence settings. Trends Organ Crim 15, 111–129 (2012). https://doi.org/10.1007/s12117-012-9159-z

of anonymity online, argued by some as a fundamental human right, but in reality an invention of the Internet - a power of invisibility that comes with great responsibility. We need to debate and discuss the increasing prevalence of cyber vigilantism[25] whereby the 'cyber pitchfork mob' act as a law unto themselves and accuse, harass, target and de-platform at will.

Profiteers in Cyberspace have to be involved in Safety and Security

Accountability and duty of care will become increasingly important, arguably involving those who profit in cyberspace in the cost of delivering on safety and security. It is essential to maintain a balance between privacy, the vitality of the tech industry and collective security; none of these entities should have primacy over the other. However, it will become progressively more challenging to deliver on collective security when there exist domains that are 'warrant proof' or effectively beyond the law. In an era of policing augmented by technology in the form of cameras, automatic license plate readers, facial recognition software, drones, Internet of Things (IoT) sensors, predictive profiling and pre-crime intervention, all operating simultaneously in the real-world and cyberspace, 'keeping the peace' has become a complicated, multi-faceted task; arguably fraught with ethical complexity in terms of privacy and civil liberties.

A Need to Re-examine the Social Contract

Therefore, police leadership, policymakers and society should explore the challenges and opportunities of existing and emerging technologies. Additionally, the social contract that has evolved over hundreds of years of policing should perhaps be re-examined and redrawn? The need for protection in technology environments should also be debated and re-evaluated. How does the thin blue line transposed to cyberspace manifest, and when conceptualising new demarcation in cyberspace where does responsibility lie in terms of maintaining secure and safe societies? Policing bodies worldwide need to work out where on the spectrum of total order and total disorder they position their activities,

25 Cyber vigilantism: "Online actions in pursuit of what is seen as justice by self-appointed individuals or groups lacking legal authority, typically when they see legal action as grossly inadequate" https://www.oxfordreference.com/view/10.1093/acref/9780191803093.001.0001/acref-9780191803093-e-1803

where they draw that blue line - considering that in cyberspace we may be heading towards disorder.[26]

When it comes to law and order parameters, we may have to reconceptualise the future of our communities and our societies, understanding what is required to ensure public safety and maintain security; to tackle online harms, anti-social behaviours and criminality, whilst at the same time accommodating evolving and changing societal values. The role of industry in developing new technologies should be re-evaluated, to ensure stakeholder inclusion and to promote an approach that is human-centric, safe and secure by design.

Police are now, more than ever, required to deliver on keeping their communities safe, in the real-world, and in cyberspace, in an ever-expanding technological upheaval where traditional policing arguably has ever-decreasing applicability, where similar to the 19th-century battlefields, resources are thinly stretched and are resisting far greater forces. This requires innovative and adaptable approaches while upholding the core principles of serving and protecting the population. Learnings from the history of policing can perhaps inform solutions, the legacy of continuous adaptation to changing circumstances, and also by innovative approaches that aim to implement the idea of community policing in cyberspace, such as *Estonia's Web Constable* concept, a dedicated group of police officers established in 2011 that are present online and respond to inquiries by citizens and provide cybersecurity advice.[27] Our collective future should not be determined by the perceived differences between officers and citizens, by an "us versus them" mentality, or by entrenched lines. Our focus should be on how we can all join forces and co-operate in the new environment of cyberspace.

The challenge may ultimately be one of societal responsibility, a social imperative to tackle evolving cyber criminality and to maximise the potential advantages of technology and cyberspace. Progress may ultimately be dependent on developing community policing online and reconceptualising a social contract now mediated by technology in terms of rules, regulations, policing and the law. In meeting these challenges, we can collaborate to conceptualise the *Cyber Blue Line* collectively and, in doing so, move towards a safer and more secure cyberspace.

26 Aiken, M. P. & Gawande, S. (2021). Nature, Structure and Science of Cyberspace: In S. Bhave (Ed.), Cyberpsychiatry. Nagpur, India.

27 https://www2.politsei.ee/en/nouanded/veebikonstaablid/

Headquartered in The Hague, the Netherlands, Europol supports the 27 EU Member States in their fight against terrorism, cybercrime and other serious and organised forms of crime. We also work with many non-EU partner states and international organisations. From its various threat assessments to its intelligence-gathering and operational activities, Europol has the tools and resources it needs to do its part in making Europe safer. In 2019, Europol supported 1 874 international operations.

EUROPOL SPOTLIGHT - THE CYBER BLUE LINE

PDF | ISBN 978-92-95220-25-6 | ISSN 2600-2760 | DOI: 10.2813/26064 | QL-AN-21-002-EN-N

Mary Aiken PhD is a Professor of Forensic Cyberpsychology in the Department of Law and Criminology at the University of East London and Adjunct Professor at the Geary Institute for Public Policy, University College Dublin, Ireland. She is a member of the Academic Advisory Board at Europol's European Cybercrime Centre (EC3).

Philipp Amann PhD is the Head of Expertise & Stakeholder Management at Europol's European Cybercrime Centre (EC3). EC3 Expertise & Stakeholder Management is responsible for assessing and acting on relevant trends and threats related to cybercrime and cyber-security.

Cite this publication: Europol (2021), The Cyber Blue Line, Europol Spotlight Report series, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu