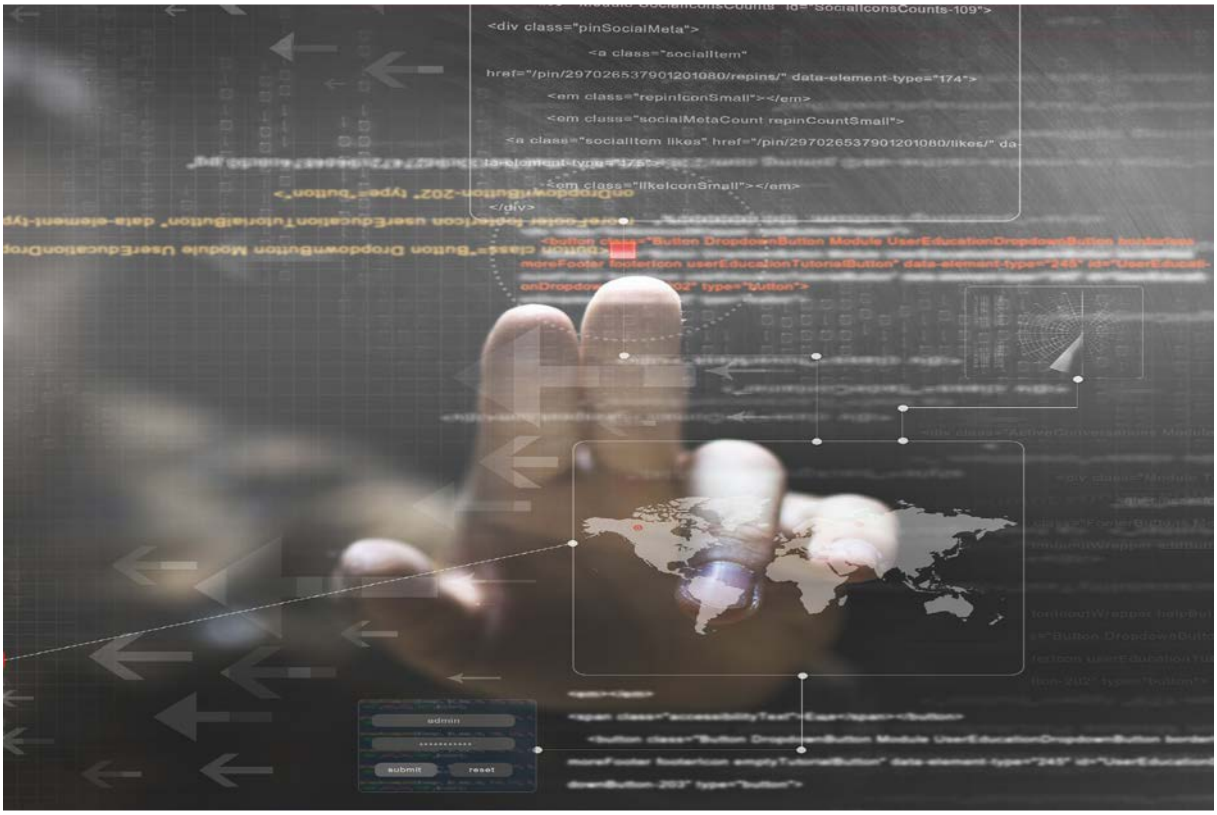
Terrorism and Cybercrime: the Human Factor



<div class="pinSocialMeta">
<a class="socialItem"
<em class="repinIconSmall"></em>
<em class="socialMetaCount repinCountSmall">
</div>
admin
submit
reset

Position Paper

May 2016

Investigating the human factor in cybercrime and terrorism

Europe faces major threats in safeguarding the security of its citizens. While registered rates of traditional crimes (burglary, car theft, shoplifting) are going down across many European nation states, Europe is increasingly facing novel crime threats, that elude national boundaries, are insufficiently understood, and therefore hard to combat or even prevent. The most pervasive and damaging of these are *cybercrime* and *terrorism*.

This position paper proposes that European research on cybercrime and terrorism be extended to better incorporate *the human factor* in studying these crimes. By the human factor we mean the impact of personal and background characteristics of perpetrators on the commission of these crimes, as well as environmental and internal factors shaping perpetrators' criminal careers (both in terms of entry and desistance) and the impact of citizen guardians in preventing, signalling, or mitigating these crimes.

Incorporating this human factor into research on cybercrime and terrorism is crucial for effective crime policies. Crime policies and discussions about policy measures are often based on implicit assumptions about offenders and offender behaviour that are seldom explicated and put to the empirical test. Strengthening sound empirical research into these assumptions will boost the quality of policy on prevention and possible interventions to create a safer Europe. Such an empirical evidence base is most urgently needed for cybercrime and terrorism/extremism: traditional sanctions for these crimes are increasingly unsuitable or unavailable: extremist attacks often end in the death of perpetrators, and cybercriminals are often outside of the reach of (supra)national justice agencies.

Cybercrime has a pervasive and massive impact. Most research so far has focused on techno-prevention of cybercrime. Very little systematic research has been conducted on the people who decide to commit these crimes: their motives, backgrounds (for instance involvement with organized crime versus lone wolves), and the impact of (para)judicial interventions and policies on their behaviour. Cybercrime has increasingly overtaken traditional crime in many European nations, and is likely to continue to expand. As so little research has been conducted on the individuals behind these crimes, it is also unknown what interventions would deter potential perpetrators nor what sanctions would reduce recidivism. As it is likely that these offenders have quite different characteristics and modus operandi than typical non-cyber offenders, past research has little to offer both in terms of theory and data. Data on these offenders have generally remained under wraps within national security agencies outside of the reach of criminologists and other social scientists.

Terrorism and other extremist acts, while very different in nature and (likely) in etiology, cause widespread destruction and suffering. Due to their high impact, their very threat can destabilize economic sectors and drain public as well as criminal justice resources. Many terrorist acts are committed by individuals whose lives – ex post facto – turn out to contain petty crime, disadvantaged socio-economic conditions, and childhood adversity. The trajectories of these criminals towards these extremely serious, often suicidal acts, and the social and economic embeddedness of their criminal careers remain, however, ill-understood: the evidence base is patchy and most petty criminals who had miserable childhoods in disadvantaged neighbourhoods do not become terrorists. Also, systemic vulnerabilities that may provide loopholes for criminal opportunities are ill-understood for these crimes. This bars prevention and targeted intervention.

Again, much knowledge remains within national security agencies; given that terrorist attacks are rare events, this implies that relevant data are scattered across Europe and no pan-European database exists to conduct analyses on, or to identify patterns from. With ongoing wars and upheaval in the Middle East and North Africa, and associated migrant flows, terrorism and right-wing activism are likely to remain a significant threat to European security.

These two different types of crimes share a number of characteristics:

- they are extremely serious and have massive consequences - stretching beyond individual victims to European defence, trade, intelligence, economy and commerce;
- they share links - albeit likely in different ways - with organized crime;
- there are no (European) sentinel data on prevalence or (characteristics of) perpetrators;
- researchers have had little access to existing police and security agency data;
- the perpetrators of these crime types are ill-understood;
- both crime types have remained understudied and theories to explain them untested.

European security research should focus on these two crime types to establish the following:

Investigate the trajectories of individuals towards the commission of these crimes

European crime and security research has so far largely overlooked the human factor in crime: studies have mainly focused on criminal structures and organizations and macro factors, but disregarded human agency. Life-course criminology studies should map patterns and factors contributing to the entry into crime, continuity, and desistance, linking specifically with the role of transnational organized crime. Once these trajectories and factors have been mapped, policies to spot offenders and intervene can be developed and the security agenda complemented. Furthermore, insight into the social and economic embeddedness of these careers and the decision making processes of these offenders will help design effective prevention strategies.

Investigate the feasibility of pan-European sentinel databases on cybercrime and terrorism

Sentinel data are essential to establish trends in cybercrime, in its interrelationships with economic crime and organized crime, and help to move away from general statements on cybercrime into more concrete understandings that could aid prevention and policing. Sentinel data on terrorism would enable to combine the spotty evidence from insular occurrences to establish patterns in offenders' steps on the radicalization path, to enable to acknowledge regional variations (e.g. Syria, IS, Maghreb, and right-wing terrorist acts). These sentinel data would have to be pan-European and projects to develop them should boost data quality and availability in many European countries. A European approach may be the only way to achieve this, as national research initiatives do not reflect the transnational nature of these crimes and will not generate access to data stored with various criminal justice and national security agencies. Constructing such a database will however need to overcome national security barriers and involve high-level cooperation.

Incorporating the human factor into research on cybercrime and terrorism is crucial for effective crime policies. Strengthening empirical research into this human factor will boost the quality of policy as well as interventions to create a safer Europe.

Marcelo Aebi (Université de Lausanne)

Catrien Bijleveld (NSCR, The Netherlands)

Felipe Estrada (Stockholm University)

Anne Getos (Zagreb University)

Edward Kleemans (Vrije Universiteit Amsterdam)

Michael Levi (Cardiff University)

Jacques de Maillard (CESDIP Paris)

Ernesto Savona (Universita Cattolica Milan)

For more information: info@nscr.nl

nscr Netherlands Institute for the Study
of Crime and Law Enforcement

www.nscr.nl