A Socio-Technical and Co-Evolutionary Framework for Reducing Human-Related Risks in Cyber Security and Cybercrime Ecosystems

Tasmina Islam[1][0000−0002−6437−8251], Ingolf Becker[2][0000−0002−3963−4743], Rebecca Posner[3][0000−0001−5744−5922], Paul Ekblom[2,4][0000−0002−6599−6174], Michael McGuire[5][0000−0002−8525−9104], Hervé Borrion[2][0000−0003−3624−4763], and Shujun Li[1](✉)[0000−0001−5628−7328]

[1] University of Kent, UK
{T.Islam,S.J.Li}@kent.ac.uk
[2] University College London, UK
{i.becker,p.ekblom,h.borrion}@ucl.ac.uk
[3] TRL Ltd, UK
rposner@trl.co.uk
[4] Central Saint Martins, University of the Arts London, UK
paul.ekblom@csm.arts.ac.uk
[5] University of Surrey, UK
m.mcguire@surrey.ac.uk

Abstract. The focus on cyber security as an interaction between technical elements and humans has typically confined consideration of the latter to practical issues of implementation, conventionally those of 'human performance factors' of vigilance etc., 'raising awareness' and/or 'incentivization' of people and organizations to participate and adapt their behavior. But this is far too narrow a view that seriously constrains the ability of cyber security as a whole to adapt and evolve to keep up with adaptive, innovative attackers in a rapidly-changing technological, business and social landscape, in which personal preferences of users are also dynamically evolving.

While there is isolated research across different research areas, we noticed the lack of a *holistic* framework combining a range of applicable theoretical concepts (e.g., cultural co-evolution such as technological arms races, opportunity management, behavioral and business models) and technological solutions on reducing human-related risks in the cyber security and cybercrime ecosystems, which involve multiple groups of human actors including offenders, victims, preventers and promoters. This paper reports our ongoing work in developing such a socio-technical framework 1) to allow a more comprehensive understanding of human-related risks within cyber security and cybercrime ecosystems and 2) to support the design of more effective approaches to engaging individuals and organizations in the reduction of such risks. We are in the process of instantiating this framework to encourage behavioral changes in two use cases that capture diverse and complicated socio-technical interactions in cyber-physical systems.

Keywords: Socio-technical · framework · Human factors · Human behavior · Risk management · Cyber security · Cybercrime · Co-evolution · Ontology · Transportation · Human-as-a-Security-Sensor (HaaSS) · Crime prevention

1 Introduction

Cyber security has increasingly become challenging for businesses, governments, the general public and society as a whole. The IBM X-Force Threat Intelligence Index 2019 [32] reported that finance and insurance, transportation, professional and health-care services were the most targeted sectors in 2018 and inadvertent human error facilitated most of the attacks and incidents. Over the years, researchers in different disciplines (e.g., computer, crime, behavioral and social sciences) have consistently identified and acknowledged the role of human behavior and human error in security incidents. According to [29], almost 90% of cyber attacks were caused by human error or behavior, but organizations often undermine the control of human-related errors and prioritize technical controls as a major remedy for security breaches [33,30]. In most cases this is due to a misconception of the term 'cybercrime', namely that it occurs purely within a non-physical (cyber) domain without any social or human-related element seen in traditional/physical crimes. At the same time, researchers are encouraging a shift in thinking where security has to work in collaboration with humans [6,42,7].

'Hyper-connectivity' [38], the unprecedented linking of individuals and technologies into vast new global social-physical networks, "opens up more points of presence for attack and exploitation" [5,35]. Due to this 'hyper-connectivity' of human and technology, the complexity and unpredictability of vulnerabilities have increased exponentially. One major approach to reducing material crime, situational prevention [12,22], seeks to reduce the opportunity for offending by altering the environment within which offenders operate so as to increase the (perceived) risk and effort to the offender, reduce (perceived) rewards and provocations and remove excuses. It however has yet to be fully applied to cybercrime and brought together with the concept of hyper-connectivity.

Likewise, ecological and evolutionary concepts can be brought in. Ecologically, in this hyper-connected cyber-physical environment, humans and corporate socio-technical agents such as businesses and organizations play various roles (e.g., offender, preventer, target, victim, etc.) and interact through conflict, cooperation, coalition, commensalism in a common 'habitat' [9,10]. This complex, non-linear process in the ecosystem can lead to co-evolution [16], for example arms races between offenders and preventers through techniques, procedures and designs [18,34]. The dynamic evolution of cyber systems is faster than in biological evolution or material culture, being based on convention and coding rather than physical necessity. Criminal techniques also continually evolve as offenders adapt to hazards and exploit opportunities [43]. Some recent work appreciates the power of evolutionary approaches in enhancing cyber security [8,14,11], but progress is fragmentary and limited.

This dynamic interactivity and co-evolution within the cyber risk ecosystem raises practical concerns, particularly how to mobilize a diverse population of individuals and organizations to support security by acting as preventers and not promoters of crime (those who inadvertently, carelessly or deliberately increase the risk of crime, e.g., by leaving their terminal unlocked or providing exploit kits). According to the CLAIMED framework reported in [17], effective mobilization requires agents with a preventer role to be alerted, informed, motivated (e.g., with incentives or regulations), empowered and perhaps directed. Such mobilization is constrained by the lack of personalization and information about dynamically evolving personal preferences at individual level.

While there is isolated research across different areas, we are not aware of any *holistic* framework combining all these theoretical approaches, e.g., co-evolution, opportunity management, behavioral and business models, with ad hoc technologies on cyber risks and specific types of cybercrime, to allow a more comprehensive understanding of human-related risks within cyber security and cybercrime ecosystems and to design more effective approaches for mobilizing individuals and organizations, and designing human-ICT systems, in the reduction of such risks. Therefore, the main aim of this paper is to present such a socio-technical framework addressing cyber security and cybercrime via a co-evolutionary approach to reduce human-related risks in the human-cyber ecosystems. The framework combines a range of applicable theories and data-driven analysis with the aim to create a computational ontology and knowledge base, which can support the design of more effective software tools to engage individuals and organizations for the reduction of human-related risks.

The remainder of this paper is organized as follows. Section 2 gives a brief review of some selected related work. The main body of this research is presented in Section 3, where we describe the proposed framework and the research approaches chosen. This is followed by an architectural overview of our work (Section 4), and two use cases that instantiate the framework to change human behavior to reduce cyber risks (Section 5). We conclude the paper in Section 6.

2 Related work

This section presents a brief review of some selected relevant research studies and projects.

Many cyber security attacks are caused by human errors and attackers are focusing more on exploiting human vulnerabilities [29,21,32]. Therefore, understanding human roles in supporting cyber security is becoming more important. Joinson and van Steen suggested integrating culture, behavior and the design of security tools and policies for this purpose [28].

Dykstra and Orr proposed a human decision analysis framework to identify the risk context and the appropriate response type in complex situations [15], and Ganin et al. proposed a multicriteria decision framework which integrates risk assessment (threat, vulnerability and consequences) for prioritizing countermeasures through user-friendly software [23].

The co-evolutionary aspect of cyber security and its potential benefits (in terms of allowing a more dynamic, 'naturalistic' response to system threats) have not been widely researched to date. Where this concept has been examined the work has largely involved algorithmically driven approaches. For example, the "Co-evolutionary Agent-based Network Defense Lightweight Event System" (CANDLES) discussed in [41] is "a framework designed to co-evolve attacker and defender agent strategies and evaluate potential solutions with a custom, abstract computer network defense simulation". By utilizing a qualitative analysis of the result data, the aim was to provide a proof of concept for the applicability of co-evolution in planning for, and defending against, novel attacker strategies in computer network security. This focuses upon fairly limited, exclusively software-focused co-evolution in cyber security.

The situational approach to the causation and prevention of crime originated in the material world. Research links to cybercrime have been limited (e.g., see [37,13]), although this is now changing [27], and the United Nations Office on Drugs and Crime has recently developed educational modules connecting these approaches[6]. Equally rare are socio-technical approaches to crime, as social and technological research have tended to operate in separate cultural silos (see e.g. [36]); exceptions based on cultural/technological co-evolution include work reported in [18] (terrorism) and [19] (crime).

As a special area of cyber security that requires a more holistic approach, a lot of work on privacy protection has considered a socio-technical approach, but as far as we know the co-evolutionary aspect has not been considered. In the following, we briefly introduce some related work in this area.

Robol et al. reported their work towards building data protection law compliant socio-technical systems [40], focusing on the new EU GDPR (General Data Protection Regulation). They utilize a goal based modeling language that allows the modeling of "social aspects of the GDPR, such as, the relationship between data subjects, data controllers, data processors, employer, and employees, in the context of personal data processing" to automatically verify privacy policies. Similarly, Raschke et al. [39] reported a design and implementation of a GDPR-compliance related privacy dashboard addressing the requirements of the GDPR and enabling users to execute data privacy rights with the tool.

In 'Privacy Flag' [3], a European Commission funded research project, crowdsourcing based mechanisms are considered for identifying, monitoring and assessing privacy-related risks, in combination with ICT technologies and legal expertise on data protection laws such as GDPR. Privacy risks are identified by distributing privacy monitoring agents on users' smart phones and websites. Users are made aware about identified risks by being informed about the risks when they are using different computer applications.

Another European research project, 'OPERANDO' (Online Privacy Enforcement, Rights Assurance and Optimization) [1], enables the Privacy as a Service (PaS) business paradigm and the market for online privacy services by implementing and exploiting an innovative privacy enforcement platform. An impor-

[6] https://www.unodc.org/e4j/en/tertiary/cybercrime.html.

tant aspect of this project is to provide a simple privacy dashboard for end users, allowing them to control their privacy settings in their regularly used platforms. A tool called PlusPrivacy [2] has been launched as a web or smart phone app as part of the OPERANDO project, which allows users to specify their privacy preferences in online social networks, for purposes such as blocking ads, malware, tracker, unwanted apps or extensions, and hiding their email identities [24].

The aim of yet another European research project 'SPECIAL' (Scalable Policy-aware Linked Data Architecture For Privacy, Transparency and Compliance) [4] is to develop technologies that collect proper consents for data and metadata in order to enable secure and privacy respecting workflows. A particular focus of this project is on data processing in big data environments where individuals' privacy choices are often neglected.

From the above brief review of related work, we can see that, although there are isolated socio-technical works on addressing human-related risks in cyber security, there is no holistic framework that allows a more comprehensive understanding of human-related risks within cyber security and cybercrime ecosystems and enables the design of more effective approaches for engaging individuals and organizations in the reduction of such risks. Particularly, the co-evolutionary aspect is not well considered in the literature. Our proposed framework in this paper will help fill this gap.

3 Methodology

Our proposed framework is built around four aspects we consider important:

- Cyber security and cybercrime are better viewed as *dynamic* processes, so applying an approach based on learning/development and cultural co-evolution will facilitate our understanding and help generate best interventions amid diverse contexts and over a sustained period during which offenders are simultaneously seeking to develop countermeasures.
- Human-related risks in cyber security and cybercrime ecosystems can be better understood if the concept of cyber-physical *hyper-connectivity* is applied to expose more complicated interactions among different stakeholders occupying diverse crime-related roles, environmental factors, events and consequences.
- *Personalization and contextualization* can help better *incentivize* people and organizations to adapt their behaviors towards reduced cyber risks and victimization rates and at the same time glean more accurate information to better understand those behaviors.
- Theoretical concepts from social psychology and cultural evolution, and computational software tools can be combined to form a *socio-technical* framework applicable to real-world cyber security and cybercrime use cases.

To address these aspects we adopt a hybrid (top-down and bottom-up) approach combining both theory and data-driven analysis (see Sections 3.1 and 3.2). We are developing an ontology of the risk ecosystem (see Section 3.3)

to facilitate computational approaches to handling the dynamics of interactions between offenders, preventers, promoters, responders and victims over various timescales and a socio-technical framework to foster practical implementations that can benefit end users directly (see Section 3.4). Our methodology is visualized in Fig. 1, and the following sub-sections will explain different parts of the methodology.

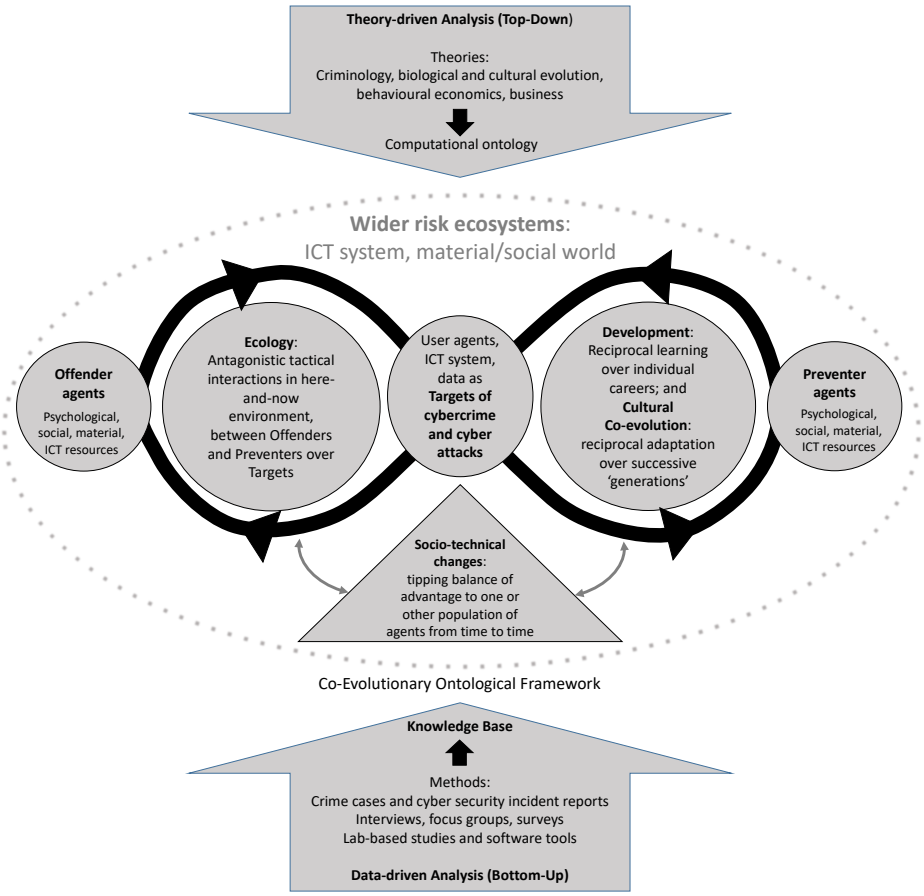

Fig. 1. The general methodology of our research towards a socio-technical and co-evolutionary framework for reducing human-related risks in cyber security and cybe-crime ecosystems.

3.1 The Top-Down Approach

This approach incorporates theoretical concepts from social, biological and behavioral sciences that provide useful insights into the co-evolutionary aspect of

cyber security and cybercrime ecosystems. That is, how cyber attackers ('predators'), victims ('prey'), security service providers and law enforcement ('preventers') constantly and dynamically adapt their behaviors in response to each other within the ecosystems involving information technology, interactions among people and organizations, regulations and policies.

A computational ontology is needed to capture such theoretical concepts to allow software tools to make use of them. To this end, we are developing such an ontology to identify the key agents and processes within cyber security ecosystems. This is especially important where analyzing problems and devising solutions involving computational approaches. More details of the ontology are given below in Section 3.3.

3.2 The Bottom-Up Approach

In this approach extensive real-world data is drawn from different sources on behaviors of individuals (with different roles) and public/private organizations within cyber security and cybercrime ecosystems. Data is collected through a combination of social methods (e.g., ethnographic interviews and surveys, focus group interviews, and psychometric testing sessions) and technological ones (e.g., automated data collection and behavioral monitoring, (semi-)automated data analytics, and data mining), in order to gather the ethnographic and behavioral information needed to build a cyber security and cybercrime knowledge base.

Combining the computational ontology with the knowledge base, we can build software tools that can understand cyber security and cybercrime ecosystems especially behaviors of stakeholders (individuals and organizations) better. This will allow more intelligent tools to help stakeholders (victims and preventers) to better respond to cyber attacks and cybercrime, hopefully helping them win (or at least keep up in) the arms race against cyber attackers and criminals.

3.3 Ontology

Originally a term in traditional philosophy, 'ontology' is now used to refer to a formal naming and definition of types, properties, and inter-relationships of entities that exist for a particular domain of discourse in science, practice or in this case, both. Ontologies have been heavily used within computer science because of the need for coding concepts and coding language that is clear enough to be represented conceptually and computationally. To make co-evolutionary processes tractable for modeling within a cyber security and cybercrime context, three fundamental aspects of interaction between agents (i.e., individuals, organizations, and intelligent software technologies) and environments in which they behave, operating over successively longer timescales, were identified as the basis for the proposed ontology.

Before giving more details of our proposed ontology, let us clarify what some key terms mean. 'Agency' could be vested in individuals, groups, organizations and intelligent software. 'Environment' includes the cyber and or social environment, as well as other agents who may be potential victims or third parties,

and either hostile or supportive. Indeed, to cope with the messy complexity of social and commercial life, agents are best described through roles. Crime roles include 'offenders' (who are doing the cyber attack), 'preventers' (who aim to reduce the risk, whether to themselves as potential victims or to third parties), 'promoters' (who increase the risk of crimes committed by others, whether accidentally, carelessly or deliberately) and 'victims' (who are adversely affected by the cyber crime) [20]. Responders act after the crime, to limit or mitigate any harm, or pursue offenders. 'Civil' roles of concern to us include at least end users, employees, managers, and system designers. Any civil role can overlap with any crime role, e.g., an agent could be both a system designer and a crime promoter if the software designed is insecure. 'Opportunity', and its exploitation, creation and denial, could equally be from the perspective of the offender, or that of security [19] — indeed, the offender's opportunity is the security manager's problem (e.g., the situational context of an attempted breach and a successful/unsuccessful security response to this), and vice-versa.

Our ontology includes three core elements: Ecology (ECO), Development (DEVO), Evolution (EVO). We are in the process of developing an initial high-level ontology. In this paper, we will briefly introduce the three core elements below, and leave greater details of the ontology for another follow-up paper.

Ecology (ECO) relates to the interactions of agents within their environment, centring mainly on opportunity and using their existing repertoire of behavior and resources. In today's cyber-physical environment, agents can be described simultaneously through crime roles and 'civil' roles. The offender and preventer may be empowered by particular physical, psychological or informational resources. Civil roles overlap with the crime roles in diverse combinations. The target of cybercrime may be a human (i.e., the victim) or some physical or cyber asset; and the interaction occurs in a wider environment which may favour the offender or the preventer. The whole thing can be called the 'risk ecosystem'.

Development (DEVO) relates to the learning that individuals and organizations can achieve during their career as offenders, preventers, promoters, responders or victims[7]. This could come from solving a problem in the here-and-now that can be remembered and reproduced if it proves a useful extension of their repertoire in tackling similar challenges in later times and other contexts. Alternatively, it may be gained through social learning.

Evolution (EVO) details how the relevant agent populations generate a variety of traits, and transmit the successful ones to succeeding generations, including via active teaching and via online guides and exploit kits, and how the traits change over 'generations' in response to selection pressures (i.e., successes and failures of crime commission or prevention). Here, the emphasis is on cultural [31] or symbolic [26] evolution, which shares many properties with biological evolution but is far less constrained and canalized. Since we are concerned with progressive behaviors of individuals and organizations playing all crime roles,

[7] This is less straightforward for victim and promoter roles, as both could develop into preventers or even offenders.

and reciprocal counter-adaptations in the security arms race, co-evolution is of particular interest.

3.4 Socio-Technical Framework

Based on the hybrid approach, the ontology and the knowledge base, we can build a socio-technical framework that will work with end users and organizations in the cyber security and cybercrime ecosystems. The main idea is to combine the following three key elements to support the development of a user-centric software architecture and a tool-set (see Section 4).

1. *(Semi-)Automated behavioral sensors to reduce burden of reporting*: A major problem of existing cyber security and cybercrime reporting systems is the difficulties in engaging users and getting such reports processed manually. This is one of the reasons why system designers are often lagging behind cyber attackers and criminals. For our framework, we proposed to deploy (semi-)automated behavioral sensors on end users' computing devices in such a way that they do not need to fill a lot of rigid and lengthy forms to report cyber security incidents and cybercrime cases. The key to make this part possible in real world is to incentivize end users with tangible benefits, e.g., reduced efforts of reporting incidents and more situational awareness made possible via such behavioral sensing. Privacy should be paid special attention so that users can have full control on what such sensors are monitoring and what data are shared with what external entities for what purposes. Behavioral sensors deployed on end users' devices will still interact with the user from time to time, but such interactions will be significantly reduced. Such behavioral sensors also include passive sensors deployed as OSINT (open-source intelligence) tools so that behaviors of cyber attackers and criminals can also be collected.

2. *More personalized and contextualized responses*: With behavioral sensors deployed on the user's own devices, the system and other entities playing the role of preventers can personalize their responses to the target user and contextualize the responses according to the nature of the cyber security and cybercrime problems much more easily. This includes tailoring the incentivizing strategies following the user's set preferences and psychological profiles. The personalization and contextualization process will have human experts in the loop to overcome accuracy problems of fully automated systems.

3. *Embedded cyber security awareness and behavioral nudging in the whole process*: The behavioral sensors deployed at the user side can work with online services provided by third parties playing the crime role of preventers (e.g., IT services of organizations, law enforcement, more educated friends and family members) to better embed cyber security awareness and behavioral nudging elements into the whole ecosystem.

The whole framework has a closed feedback loop so that any new information gathered through the relevant tools will be fed back to evolve the framework and its different components accordingly, which include but are not limited to the computational ontology, the knowledge base and all the tools themselves, in addition to helping human actors to evolve. Combining with evolving people,

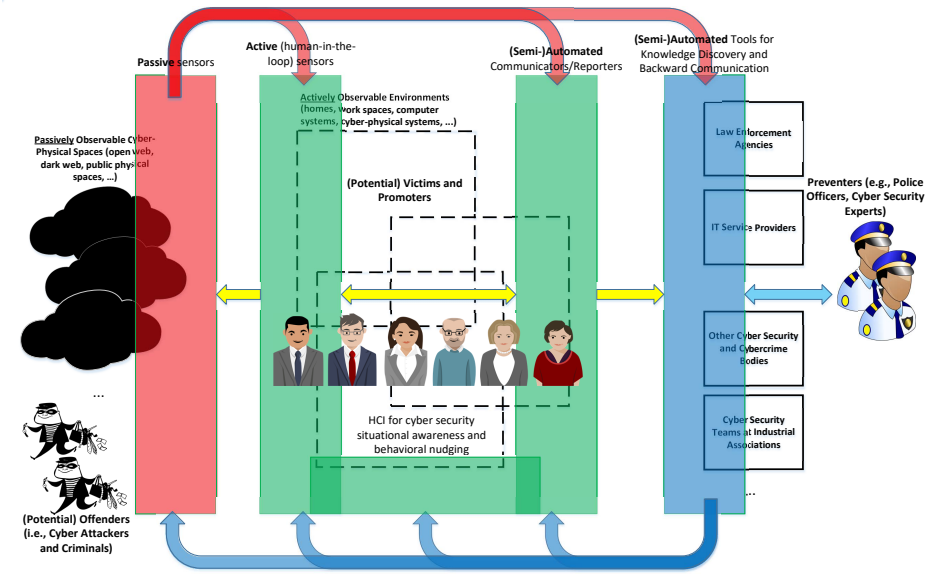

Fig. 2. The proposed socio-technical framework with a closed loop.

the framework can help improve all 'good' actors in the ecosystem to hopefully defeat 'bad' ones.

A graphical representation of the framework with a closed loop can be found in Fig. 2. It shows how different groups of human actors are involved in the framework, with (potential) offenders on the left, (potential) victims and promoters in the middle, and preventers on the right. There are three groups of arrows showing how different types of information flow within the framework: 1) red arrows representing behavioral information about offenders flowing to potential victims and preventers; 2) yellow arrows representing information of the user environments that can flow to offenders and preventers; 3) blue arrows representing information with preventers that can flow to (potential) victims, (potential) promoters, and (potential) offenders. Note that some human actors may have overlapping roles, e.g., a money mule may be both a victim and a criminal.

4 Software Framework

To implement the socio-technical framework described in Section 3.4, we need to consider how practical software tools can be developed and with what computing systems they will work. In this section, we describe a possible software framework shown in Fig. 3, which includes some user-centric software tools running from the user's own device.

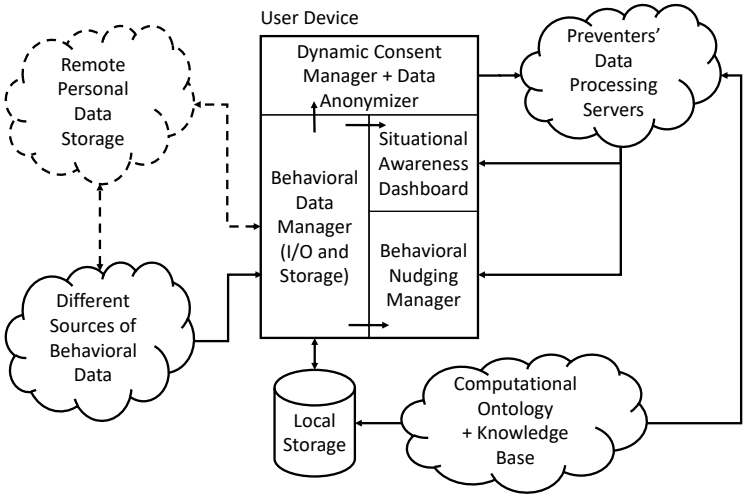

Fig. 3. A possible software framework for implementing the socio-technical framework.

The user-centric software interacts with users and external data sources to get useful behavioral data the user can see, and also with user-selected preventers for incident reporting, cyber security awareness and behavioral nudging purposes. Different data plugins are needed to support collecting data from different data sources, and they collectively form a behavioral data manager (BDM). To allow the user to manage his/her personal data shared with preventers' servers without privacy concerns, a dynamic consent manager (DCM) equipped with a data anonymizer is needed to ensure all data flowing out of the user's device are processed properly with the user's explicit consent. Behavioral data dynamically collected by the user-centric software tools can be stored either locally or on a remote personal data storage or both (e.g., the local storage can be used as an offline cache of behavioral data). A typical example of the user-centric software is a mobile app running from the user's mobile device or a web application that can run from multiple devices of the user.

The remote personal data storage may be simple cloud-based online drives, but can also be more complicated personal data management platforms (PDMPs), such as Solid (https://solid.mit.edu/), Databox (https://www.databoxproject.uk/), Hub-of-all-things (https://www.hubofallthings.com/) and digi.me (https://digi.me/), which allow users to manage their own data for multiple online services more easily. Such platforms often have an interface to allow data I/O with external software, so they can be incorporated into the user-centric software tools of our proposed framework.

The preventers' servers are also very important because they provide the needed feedback to the user. There are two main types of feedback: information for cyber security situational awareness enhancement, and information for behavioral nudging, which are processed by two separate components of the user-

centric software, situational awareness dashboard (SAD) and behavioral nudging manager (BNM). The SAD and BNM are also informed by the BDM so that some data not shared with the preventers' servers can still be considered locally to help the user.

The computational ontology and the knowledge base we explained in the previous section can be used to support both the user-centric software tools and also the preventers' servers. They can be implemented as public data that can be retrieved from different computer applications. When necessary, personal data available on the user's device can be used to personalize the computational ontology and the knowledge base, e.g., storing a reduced version relevant for the target user only. On the preventers' servers, the computational ontology and the knowledge base should be able to cover all users the preventers aim at supporting.

5 Use Cases

The software framework described in the previous section is very generic. For different user groups and contexts, different software tools will have to be implemented, although they share many common software components. This means that we need to look at concrete use cases for real-world implementations, in order to validate the effectiveness of the proposed framework. We are currently conducting research and development work on two such use cases, which we describe in the following two subsections.

5.1 Human-related security risks within hybrid transportation networks

Through the proposed framework this use case will focus on understanding the role of human behavior within an increasingly connected transport system to prevent an emerging type of cyber-physical crimes. These crimes include perpetrators collecting data through intelligent transport systems (e.g., connected vehicles or public transport systems) or transport-based apps in order to plan cyber or cyber-physical attacks on vehicles, transport systems or individuals involved (e.g., drivers and passengers).

The use case will start with investigating the values and motivations that influence location sharing behaviors of transport users (potential victims) on transport-related mobile apps as well as how these vary across different segments of the population (shown in Fig. 4). From an ecological, here-and-now perspective, we also need to understand general cyber-physical behaviors of users and offenders and how this relates to the socio-technical environment within which both parties operate and conflict with one another.

Because today's transportation networks are very complicated, there are still many different data and attacks we can consider for this use case. In order to provide a more tangible use case, we will narrow down to user behavior around sharing geolocation data, and for the offenders' side we will consider privacy

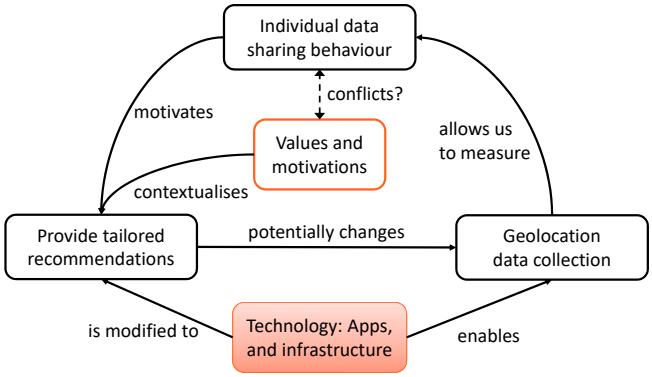

Fig. 4. Human-related security risks within hybrid transportation networks.

attacks that can be conducted based on leaked geolocation data. For preventers, we will use ourselves (cyber security researchers) to mimic different types of preventers in real world. The feedback loop will be implemented by informing the user about geolocation data shared and data consumers, and by providing concrete recommendations for the user to adapt his/her geolocation data sharing behavior to reduce privacy attacks. A number of mobile apps supporting geolocation sharing have been identified as data sources for developing behavioral sensors. We will develop a mobile app to implement the software framework described in the previous section, and human participants will be recruited to use the mobile app in order to verify if and how they will adapt their behavior due to interactions with our simulated preventers' servers.

5.2 Human-as-a-Security-Sensor (HaaSS)

This use case looks at the scenario of security attack reporting by users to IT departments of organizations or other cyber security service providers. We will look at adding a feedback loop to the Human-as-a-Security-Sensor (HaaSS) system reported in [25], in order to test if the closed-loop process can help improve human reporters' performance in reporting cyber attacks (shown in Fig. 5). Simulated social engineering attacks will be conducted in the same way as reported in [25]. Multiple rounds of user studies are planned to hopefully allow us to observe a learning or an evolutionary effect. The user-centric software and a simulated server will be developed based on the original HaaSS software system, collaborating with the authors of [25].

6 Conclusion

This paper presents a socio-technical framework for addressing human-related risks in cyber security and cybercrime ecosystems. It is a closed-loop framework, considering different human actors playing different crime roles (offenders,

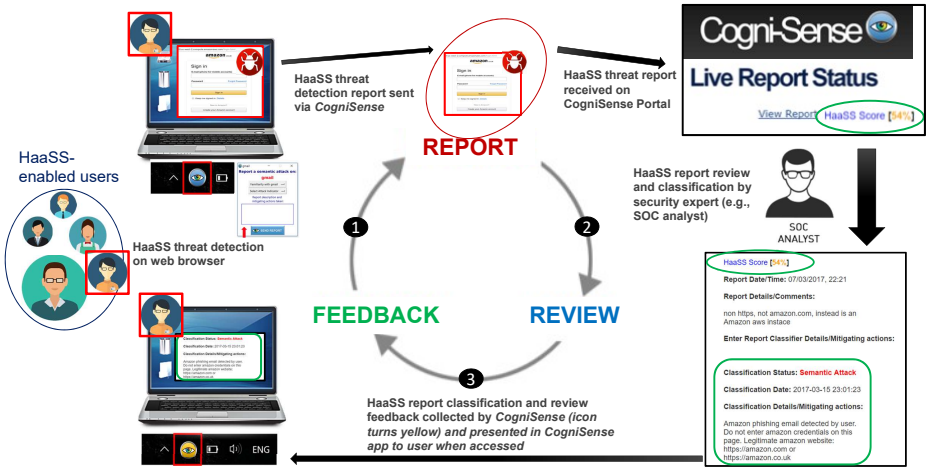

Fig. 5. Human-as-a-Security-Sensor with a feedback loop.

preventers, promoters, responders and victims). It follows a hybrid approach to combine theories and data-driven analysis, aiming at creating a computational ontology and a knowledge base that can support user-facing software tools and preventers-facing analytics at the server side. The framework has (potential) victims and promoters at the center, and employs behavioral sensing to enable more personalized and contextualized feedback from preventers for the purpose of reducing human-related attacks. We are currently working on software implementations of the framework for two use cases, and will conduct user studies to verify the effectiveness of the developed software tools on recruited human participants in simulated cyber security scenarios.

Acknowledgments

This work was supported by the research project, "ACCEPT: Addressing Cybersecurity and Cybercrime via a co-Evolutionary aPproach to reducing human-relaTed risks" (http://accept.cyber.kent.ac.uk/), funded by the EPSRC (Engineering and Physical Sciences Research Council) in the UK, under grant number EP/P011896/1 and EP/P011896/2.

References

1. Operando homepage, https://www.operando.eu/, last accessed 26 April 2019
2. PlusPrivacy homepage, https://plusprivacy.com/, last accessed 26 April 2019
3. Privacy Flag homepage, https://privacyflag.eu/, last accessed 26 April 2019
4. SPECIAL homepage, https://www.specialprivacy.eu/, last accessed 26 April 2019
5. Ablon, L., Libicki, M.C., Golay, A.A.: Markets for cybercrime tools and stolen data: Hackers' bazaar. Tech. rep., RAND Corporation (2014), https://www.rand.org/pubs/research_reports/RR610.html

6. Adams, A., Sasse, M.A.: Users are not the enemy. Communications of the ACM **42**(12), 40–46 (1999). https://doi.org/10.1145/322796.322806
7. Beautement, A., Becker, I., Parkin, S., Krol, K., Sasse, M.A.: Productive security: A scalable methodology for analysing employee security behaviours. In: Proceedings of 12th Symposium on Usable Privacy and Security. USENIX Association (2016), https://www.usenix.org/conference/soups2016/technical-sessions/presentation/beautement
8. Behdad, M., Barone, L., Bennamoun, M., French, T.: Nature-inspired techniques in the context of fraud detection. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews **42**(6), 1273–1290 (2012). https://doi.org/10.1109/TSMCC.2012.2215851
9. Bernasco, W.: Foraging strategies of homo criminalis: Lessons from behavioral ecology. Crime Patterns and Analysis **2**(1), 5–16 (2009)
10. Bichler, G., Bush, S., Malm, A.: Regulatory foresight: Estimating policy effects on transnational illicit markets. Contemporary Criminal Justice **31**(3), 297–318 (2015). https://doi.org/10.1177/1043986215575138
11. Bold, K.: Inspired by nature, researcher develops new cyber security techniques (2014), https://phys.org/news/2014-05-nature-cyber-techniques.html
12. Clarke, R.V.: Seven misconceptions of situational crime prevention. In: Handbook of Crime Prevention and Community Safety, pp. 39–70. Routledge (2013)
13. Collins, B.S., Mansell, R.: Cyber trust and crime prevention: a synthesis of the state-of-the-art science reviews. Tech. rep., Office of Science and Technology, UK (2004), http://eprints.lse.ac.uk/4252/
14. Demertzis, K., Iliadis, L.: A bio-inspired hybrid artificial intelligence framework for cyber security. In: Computation, Cryptography, and Network Security, pp. 161–193. Springer (2015). https://doi.org/10.1007/978-3-319-18275-9_7
15. Dykstra, J.A., Orr, S.R.: Acting in the unknown: The Cynefin framework for managing cybersecurity risk in dynamic decision making. In: Proceedings of 2016 International Conference on Cyber Conflict. pp. 1–6. IEEE (2016). https://doi.org/10.1109/CYCONUS.2016.7836616
16. Ehrlich, P.R., Raven, P.H.: Butterflies and plants: A study in coevolution. Evolution **18**(4), 586–608 (1964). https://doi.org/10.1111/j.1558-5646.1964.tb01674.x
17. Ekblom, P.: Crime prevention, security and community safety using the 5Is framework. Springer (2010). https://doi.org/10.1057/9780230298996
18. Ekblom, P.: Terrorism: lessons from natural and human co-evolutionary arms races. In: Evolutionary Psychology and Terrorism, pp. 82–113. Routledge (2015)
19. Ekblom, P.: Crime, situational prevention and technology: The nature of opportunity and how it evolves. In: The Routledge Handbook of Technology, Crime and Justice, pp. 379–400. Routledge (2017)
20. Ekblom, P.J.: Conjunction of criminal opportunity theory. Encyclopedia of Victimology and Crime Prevention (2010). https://doi.org/10.1057/9780230298996
21. Evans, M., He, Y., Maglaras, L., Janicke, H.: HEART-IS: A novel technique for evaluating human error-related information security incidents. Computers & Security **80**, 74–89 (2019). https://doi.org/10.1016/j.cose.2018.09.002
22. Freilich, J.D., Newman, G.R.: Situational Crime Prevention, vol. 1. Oxford University Press (2017). https://doi.org/10.1093/acrefore/9780190264079.013.3
23. Ganin, A.A., Quach, P., Panwar, M., Collier, Z.A., Keisler, J.M., Marchese, D., Linkov, I.: Multicriteria decision framework for cybersecurity risk assessment and management. Risk Analysis (2017). https://doi.org/10.1111/risa.12891

24. Grace, P., Surridge, M.: Towards a model of user-centered privacy preservation. In: Proceedings of 12th International Conference on Availability, Reliability and Security. p. 91. ACM (2017). https://doi.org/10.1145/3098954.3104054
25. Heartfield, R., Loukas, G.: Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. Computers & Security **76**, 101–127 (2018). https://doi.org/10.1016/j.cose.2018.02.020
26. Jablonka, E., Lamb, M.J.: Evolution in Four Dimensions, Revised Edition: Genetic, Epigenetic, Behavioral, and Symbolic Variation in the History of Life. MIT Press (2014)
27. Johnson, S.D., Ekblom, P., Laycock, G., Frith, M.J., Sombatruang, N., Valdez, E.R.: Future crime. In: Routledge Handbook of Crime Science, chap. 30. Palgrave Macmillan (2018)
28. Joinson, A., van Steen, T.: Human aspects of cyber security: Behaviour or culture change? Cyber Security: A Peer-Reviewed Journal **1**(4), 351–360 (2018)
29. Kelly, R.: Almost 90% of cyber attacks are caused by human error or behavior (2017), https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/
30. Kraemer, S., Carayon, P., Clem, J.: Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security **28**(7), 509–520 (2009). https://doi.org/10.1016/J.COSE.2009.04.006
31. Laland, K.N.: Darwin's Unfinished Symphony: How Culture Made the Human Mind. Princeton University Press (2017)
32. Lee, C., Iesiev, A., Usher, M., Harz, D., McMillen, D.: IBM X-Force Threat Intelligence Index 2019. Tech. rep., IBM security (2019), https://www.ibm.com/downloads/cas/ZGB3ERYD
33. Liginlal, D., Sim, I., Khansa, L.: How significant is human error as a cause of privacy breaches? an empirical study and a framework for error management. Computers & Security **28**(3-4), 215–228 (2009). https://doi.org/10.1016/j.cose.2008.11.003
34. Magliocca, N.R., McSweeney, K., Sesnie, S.E., Tellman, E., Devine, J.A., Nielsen, E.A., Pearson, Z., Wrathall, D.J.: Modeling cocaine traffickers and counterdrug interdiction forces as a complex adaptive system. Proceedings of the National Academy of Sciences **116**(16), 7784–7792 (2019). https://doi.org/10.1073/pnas.1812459116
35. McGuire, M.: Hypercrime: The new geometry of harm. Routledge-Cavendish (2007)
36. McGuire, M.: Technology crime and technology control: contexts and history. In: The Routledge Handbook of Technology, Crime and Justice. Palgrave Macmillan (2016)
37. Newman, G.R., Clarke, R.: Superhighway Robbery: Preventing E-commerce Crime. Willan (2003)
38. Quan-Haase, A., Wellman, B.: Local virtuality in an organization: Implications for community of practice. In: Communities and Technologies 2005: Proceedings of the Second Communities and Technologies Conference, Milano 2005, pp. 215–238. Springer (2005). https://doi.org/10.1007/1-4020-3591-8_12
39. Raschke, P., Küpper, A., Drozd, O., Kirrane, S.: Designing a GDPR-compliant and usable privacy dashboard. In: Privacy and Identity Management. The Smart Revolution: 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Ispra, Italy, September 4-8, 2017, Revised Selected Papers. IFIP Advances in Information and Communication Technology, vol. 526, pp. 221–236. Springer (2017). https://doi.org/10.1007/978-3-319-92925-5_14

40. Robol, M., Salnitri, M., Giorgini, P.: Toward GDPR-compliant socio-technical systems: Modeling language and reasoning framework. In: The Practice of Enterprise Modeling: 10th IFIP WG 8.1. Working Conference, PoEM 2017, Leuven, Belgium, November 22-24, 2017, Proceedings. Lecture Notes in Business Information Processing, vol. 305, pp. 236–250. Springer (2017). https://doi.org/10.1007/978-3-319-70241-4_16
41. Rush, G., Tauritz, D.R., Kent, A.D.: Coevolutionary agent-based network defense lightweight event system (CANDLES). In: Proceedings of the Companion Publication of the 2015 Annual Conference on Genetic and Evolutionary Computation. pp. 859–866. ACM (2015). https://doi.org/10.1145/2739482.2768429
42. Sasse, M.A., Brostoff, S., Weirich, D.: Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. BT Technology Journal **19**(3), 122–131 (2001). https://doi.org/10.1023/A:1011902718709
43. Wortley, R.: Affordance and situational crime prevention: Implications for counter terrorism. In: Terrorism and Affordance: New Directions in Terrorism Studies, chap. 2, pp. 17–32. Bloomsbury Publishing (2012). https://doi.org/10.5040/9781501301155.ch-002