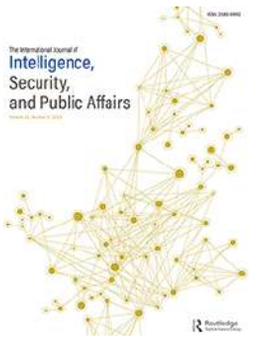

The International Journal of Intelligence, Security, and Public Affairs

ISSN: 2380-0992 (Print) 2380-100X (Online) Journal homepage: https://www.tandfonline.com/loi/usip20

Manipulation through Online Sexual Behavior: Exemplifying the Importance of Human Factor in Intelligence and Counterintelligence in the Big Data Era

Matthieu J. Guitton

To cite this article: Matthieu J. Guitton (2019) Manipulation through Online Sexual Behavior: Exemplifying the Importance of Human Factor in Intelligence and Counterintelligence in the Big Data Era, The International Journal of Intelligence, Security, and Public Affairs, 21:2, 117-142, DOI: 10.1080/23800992.2019.1649122

To link to this article: https://doi.org/10.1080/23800992.2019.1649122

Published online: 14 Aug 2019.

THE INTERNATIONAL JOURNAL OF INTELLIGENCE, SECURITY, AND PUBLIC AFFAIRS
2019, VOL. 21, NO. 2, 117–142
https://doi.org/10.1080/23800992.2019.1649122

Routledge
Taylor & Francis Group

Manipulation through Online Sexual Behavior: Exemplifying the Importance of Human Factor in Intelligence and Counterintelligence in the Big Data Era

Matthieu J. Guitton[a,b]

[a]Faculty of Medicine, Université Laval, Quebec City, QC, Canada; [b]CERVO Brain Research Centre, Quebec City, QC, Canada

ABSTRACT

As we spend more and more time online, Internet-based virtual spaces are becoming a central component of our daily life and activities. This shift of human activities from offline to online spaces has major impacts for national security. Consequently, cyberspace became a new field of operation for intelligence and counter-intelligence services worldwide. While massive efforts are made to further strategies based on surveys and analyses of large datasets, cybersecurity protocols can be impacted tremendously by individual behaviors. This is particularly the case of online sexual behavior, which can be easily manipulated by malevolent agents. This paper will describe some of the general characteristics of sexual cyberbehaviors. We will then identify some of the main threats related to sexual cyberbehavior (specifically risks of blackmailing, risks associated with the use of online dating sites, and risks associated with the consumption of online pornography), as well as the main targets in terms of population from an intelligence/counter-intelligence perspective. Finally, we will propose some possible counter-measures, that could be implemented to reduce the security risks related to online sexual behavior.

KEYWORDS

Blackmailing; counter-intelligence; intelligence; online dating applications; online dating sites; online pornography; online sexual behavior; sexual scandal

Introduction

From the alleged attempts of online manipulations of voters' opinions during the last US Presidential elections, to the recent arrest of the deputy chairwoman of the board and chief financial officer of the Chinese telecom giant Huawei in Canada at an extradition request of the United States (Fife, 2018), the media are here to remind us the critical importance that information technology have now reached for national security (Guitton, 2019b). Cyberattacks have long left the realm of fiction and cybersecurity is now a reality for intelligence and counterintelligence services worldwide. Contemporary intelligence strategies nowadays systematically include cybersecurity procedures in their repertoire. Quite logically, intelligence services

CONTACT Matthieu J. Guitton matthieu.guitton@fmed.ulaval.ca Institut Universitaire en Santé Mentale de Québec, 2601 Chemin de la Canardière (F-6500), Quebec City, QC G1J 2G3, Canada

Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/usip.

are trying to develop efficient responses and appropriate countermeasures. Massive efforts are invested in the hardware/software aspects. Thanks to the increases in calculation power, big data and artificial intelligence (AI) are in the center of the research efforts in the field of cyber-defense. When applied to online behavior, these large-scale analysis strategies can greatly service the understanding of mass behavior. For instance, analyses of large datasets of digital footprints can probe the impact of the adaptation of persuasive messages to the psychological characteristics of large groups (Matz, Kosinski, Nave, & Stillwell, 2017).

Although the questions and challenges related to the exploitation of big dataset of user profiles are without doubt of major concern, this should not shadow the importance of individual human behaviors in processes of leak of information. Indeed, although general patterns might emerge from large-scale analyses, this tends to make us forget that individuals are all unique beings and that multiple factors can affect the actualization of an individual's behavior at any given time. Without attempting here to judge the moral validity of whistleblowers, Edward Snowden should be a sufficient example for those who would need to get convinced about the devastating effects that the behavior of a single individual can have on security protocols (Lahneman, 2016). Some areas of human behavior are highly susceptible to inter-individual variability. This is particularly the case of online sexual behavior.

From Mata Hari to Katerina Leung or Anna Chapman, sex-based manipulations have always been part of the espionage world. The use of seduction and sexual activities to conduct espionage – something referred to as "sexpionage" – is part of the toolbox of most major intelligence services (Bower, 1990), some countries such as the former Soviet Union having made a heavy use of it (Lewis, 1976). Yet, the digital age might potentially propel sexpionage to a new level. Indeed, the vulnerability of individuals to sexual blackmail and the lack of predictability of individual cyberbehavior make cyberthreats associated with online sexual behavior particularly worrying. While conventional methods of individual-centered information gathering were requiring physical contacts in the real world, the digital age allows spies and other agents to operate at distance, potentially establishing fake romantic relationships while staying in their country of origin, out of the reach of counter-intelligence services. Exploring the ways manipulation of people can be done through online sexual behavior is entering a journey through the relations between intelligence and the dark net. Espionage is not about spies, it is about gathering information. Through online sexual manipulation, intelligence specialists can access numerous targets, and leverage their shadowy influence through the threat of dishonor or public shaming. Hence, manipulations through online sexual behavior emphasis the multiplicity of issues that intelligence practices are facing. The analysis we propose here will describe some of the general characteristics of sexual cyberbehaviors. We will then identify the main cyberthreats related to sexual behavior, as well as the main targets in

terms of population from an intelligence/counter-intelligence perspective. Finally, we will propose some possible counter-measures which could be implemented to reduce the security risks related to online sexual behavior.

General characteristics of sexual cyberbehaviors

Although they are influenced by individual characteristics such as age, motivations, or personality, sexual cyberbehaviors are a facet of online behavior. As such, they follow the general rules of cyberbehavior. In this context, a few characteristics of online behavior are particularly important to understand how online sexual behavior can be used to manipulate individuals for intelligence purposes.

Perceived separation between professional and private life

The first element to take into consideration when considering sexual cyberbehaviors is the perceived separation between professional and private life. The way people will behave when they are with their close friends (personal context, high emotional charge) is obviously not the same than when they are with a potential employer (professional context, high rationalized charge). As personality characteristics provide some degree of consistency to human behavior, the fact that people act differently when in different context is not due to change of personality but rather to change in attitude and intentions (Anderson & Agarwal, 2010). Indeed, individuals adapt their behavior as a function of trust, i.e., as a function of the degree of perceived vulnerability and risks. These variations of behavioral attitudes depending on the levels of perceived risks are well known and have been extensively documented, notably in the context of online purchases (McCole, Ramsey, & Williams, 2010; Park & Kim, 2003; Ratnasingham, 1998). Furthermore, through the existence of avatars, virtual spaces offer people the opportunity to simultaneously maintain different identities (Guitton, 2011, 2012; Taylor, 2002). Rather than different persona, this should instead be considered as differential actualizations of one's identity through a behavioral continuum.

From the perspective of security, trust-dependent variations in behavioral attitudes translate for an individual in maintaining different levels of vigilance. While this is true in offline life, the potential consequences in terms of security gets even more problematic in online spaces. In the context of performing their professional duties, individuals are highly aware of the issues related to information leak. Modern days professionalism in key positions emphases expert skills will include state-of-the-art security behavior when it comes to online activities. However, people tend to be much less aware of the security threats when they have online behavior related to their private and personal life rather than their professional activities. Consequently, the intensity of the cybersecurity behavior drops drastically when moving into the private domain. For instance, these

Table 1. Degrees of self-controlled behavioral standard of security.

		Setting	
		Professional	Personal
Modality	Offline	High	Intermediate
	Online	Intermediate	Low

differences can occur in browsing behavior, in the presence and activity on social media (examples are numerous of professionals having put themselves or their company in trouble by posting problematic material on their personal social media account), or in the modalities of access (accessing Internet only trough secured computers and networks for professional activities vs, accessing Internet in public places for personal online activities).

This diminution of the self-imposed levels of vigilance of an individual varies alongside two dimensions: the offline/online nature of the activities on the one hand, and professional/private domains on the other hands (Stanton, Stam, Mastrangelo, & Jolton, 2005; Thompson, McGill, & Wang, 2017; van Schaik et al., 2017). The resulting area of vulnerability in terms of cybersecurity is a potentially weak link in the security protocols (Table 1). This weakness can be readily exploited in an intelligence context of information gathering. Indeed, although the different online contexts and identities can be perceived as separated by the user, they are obviously not. A status of "friend" through a social network provides a considerable access to a wide range of personal information personal, but also to some information with professional relevance. Furthermore, knowledge related to the private life of a key person is likely to provide information that would be extremely useful for identity thieves or other password penetration purposes (e.g., date of birth, marital status, information on the partner, number and name of children).

Although this problem is well known by cybersecurity experts and is not specific to sexual behavior, this becomes particularly salient in this particular category of online behavior. Indeed, it is for this exact category of activities that the perception of this separation between work and private life is maximal. Using online dating services, sites or applications is by definition made following a personal, self-triggered process. Thus, users are not predisposed to think that they could themselves be a target during this process. With the increasing use and normalization of sexting, such situations are likely to be more and more common in the near future, with all the risks in term of breach of security consecutive to such behavior.

Hidden behaviors

In contrast to the vast majority of online activities (searching and browsing activities, social media activities, and so on), online sexual activities are inherently hidden. Largely due to socio-cultural pressure, individuals doing

such online activities are unlikely to display them publically. That being said, the Internet allows consumption of sexually explicit material by categories of population which would have typically refrain themselves to do so publically. For instance, the inverse relationship between internal and external religiosity and regular Internet pornography use has been demonstrated to be only very weak (Baltazar, Helm, McBride, Hopkins, & Stevens, 2010). Although the public perception of sexual activities has considerably evolved in the last decades, people having non-conventional sexual practices (e.g., alternative sexual practices such as those gathered under the BDSM acronym) are still the regular target of public disapprobation and shaming (Guitton, 2019a). Online adult activities are still associated with a fear of damage to the reputation – which can obviously translate into damages to the professional career. Online spaces provide a perfect venue to answer the perceived need of anonymity related to online adult material consumption.

Social pressure is still powerful, and people might go to great length to hide their online sexual behavior. A blatant example can be found in the UK with Theresa May's former First Secretary of State and Minister for the Cabinet Office Damian Green (Stewart, 2017). In December 20, 2017, Damian Green was forced to resign from his position in the Cabinet after admitting that he had lied about the presence of pornographic material on his computer at the House of Commons. It is important to note here that the issue was not Damian Green's consumption of pornography, but the fact that he was lacking of "honesty" – one of the core principles of the British ministerial code of conduct – by lying about it. Albeit it should be noted that the material found was made of legal pornography and not of material for which ownership or viewing would be criminal *per se*, Green maintained a communication strategy based on deny. The consequences for Green were much worse than if he would have admitted being aware of the presence of these pornography images on his computer.

This kind of behavioral strategies aiming at hiding online sexual activities has consequences in terms of security. Indeed, this makes the users more vulnerable to potential manipulations – blackmailing being obviously the first one coming in mind. It also prevents discussions among peers or co-workers, which could help identify online encounters as suspicious. Finally, it prevents the identification of individuals "at risk" of taking actions potentially dangerous in terms of cybersecurity, and to propose them adequate support to avoid breaks of cybersecurity to happen.

Nature of digital footprints

In contrast to an analogic logic, the cyberspace is first and foremost a digital space. Thus, each action taking place in the cyberspace is transformed to be encoded into a digital signal. Consequently, all the actions and interactions

taking place in virtual spaces can be – and in fact are – recorded. Everyone knows that any material posted on social network could be found even years after the initial publication – and a lot of people experienced embarrassing situations due to some message of photo that had been posted at some point in the past and forgotten. Each of these unnoticed evidence of our digital actions – which are known as digital footprints – contribute to draw for each individual a coherent and long-lasting identity (Saramäki et al., 2014).

Digital footprints are not alimented only by the individuals themselves. Indeed, monetary or commercial transactions, third-person report in news or social media, or incidental appearances in others activity flows all leave data which and conglomerate and aggregate in the cyberspace to form not only a unique signature for an individual, but quite a complete picture of his life and interests. Given their richness, these footprints can be exploited by those willing to find critical information on someone. Digging such data does not have to be illegal – as a matter of fact, marketing firms are doing that on a daily basis. The interest of these footprints is of course major for intelligence and counterintelligence services. Schematically, digital footprints can be separated within two categories: on the one hand. "items" (i.e., individual pieces of information, static data), and on the other hand, "network activities" (i.e., information related to connectivity and dynamics of interactions). Although a systematic analysis of all available data would be highly time-consuming, strategies based upon anomaly detection can be quite efficient, as anomalies in social networks are often the signature of abnormal, illicit, or at the very less suspicious behavior. Of note, such procedure of anomaly detection in online social network can easily be automated. The rise of AI will only increase this phenomenon and multiply the possibilities to extract information on individuals from large online interactomes (Bindu, Santhi Thilagam, & Ahuja, 2017; Lahneman, 2016). These digital footprints, which are already heavily exploited for security purposes by police forces across the world, are also of essential importance for intelligence agencies. For instance, either the lack of digital footprints, or at the other end of the spectrum, the presence of incongruence in digital footprints is strong elements used to unmask undercover identities (Lord, 2015). Big data aggregation strategies can push the analysis of digital footprints further, allowing for faster and more powerful semi-automated in-depth analyses (Bindu et al., 2017; Lahneman, 2016). From possibilities to cross-check information to possibilities to identify potential individual weaknesses of an individual, digital footprints represent an invaluable tool for any intelligence officer. In an intelligence or counterintelligence context, identifying non-conventional sexual behavior or interest of an individual obviously represents priceless information, which could easily provide some ground for blackmail or contact attempts.

In a context of manipulation through only sexual behavior, two situations have to be considered when it comes to digital footprints: the digital footprints left by operational agents, and the digital footprints left by potential targets. When compared to some other forms of cyberattacks, the digital footprints left by agents involved in manipulations based upon online sexual behaviors are considerably more difficult to exploit. This does not mean that these activities leave quantitatively less digital footprints than some other forms of cybercriminality. Instead, the difference here is qualitative: it is much more difficult to exploit these digital footprints in a meaningful way. If we take the case of online dating as an example, several elements make conventional digital footprints analysis strategies mostly irrelevant – even when assisted by the most state-of-the-art big data methods and tools. For instance, in the case of online dating, identities used by intelligence agents don't have to be necessarily fake. Indeed, a real identity could easily be used – especially for students and other young adults. Also, due to the nature of online dating, profiles used on online dating sites and applications will likely provide only very partial information (e.g., real address are unlikely to be displayed to avoid stalking), and will presumably use some degree of pseudonymous identity – yet without necessarily the abnormal patterns of activity which would be typically observed for social media bots. Thus, typical and well-known suspicious patterns in social networks such as star/near-star and clique/near-clique patterns (Bindu et al., 2017) might not be as apparent in such situation. Such behavior would be expected from any user of such sites or services with minimal concerns about his or her own (cyber)security. Hence, the lack of information or history of the real-life identity related to an online dating profile would not necessarily raises a red flag in terms of security threat, or equates a false identity.

The situation is quite the opposite when it comes to the potential targets. Indeed, and in contrast to what can be observed for online intelligence agents, the digital footprints left in the context of online sexual behavior by individuals which could potentially become targets are quite numerous. As we mentioned above, displaying any form of behavior online systematically creates associated footprints. From browsing history to specialized profiles, all these scattered information can be potentially used as weapons for reputation damage or even blackmail. Furthermore, in addition of being numerous, these footprints are relatively easy to spot. Indeed, by definition, when involved in online sexual activity, users will have to provide in the application enough information related to their offline identity so that they can be recognized as legitimate interlocutors – and even sometimes properly identified – by their expected sexual partners. Of note, the term "sexual partner" has here to be understood in a broad sense, including for instance romantic partners, but also potentially individuals sharing similar interests in the case of online adult communities. Even if users might believe that they

are hiding behind an avatar, information such as IP address, coupled quite often by real photos, are enough to allow anyone with basic knowledge of computer science to locate the person.

Identifying the threats

Whether offline or online, human sexual behaviors are diverse – and so are the related threats. Intelligence aims at gathering information, and online spaces offer the possibility for intelligence services to directly access individuals potentially holding sensitive information, without having to first secure real-life contacts with these individuals. The following paragraphs will explore three examples of intelligence-relevant cyberthreats related to online sexual behavior: blackmail, threats related to the use of online dating applications, and threat related to the consumption of online pornography.

Blackmail

Blackmailing is a practice as old as the spying profession itself. Either to gain influence or to gather information, 'chantage' has always been part of the toolbox of espionage. Yet, blackmail takes a fully new dimension in the age of the Internet. What was once an art has now becomes as easy as child play. Blackmail 2.0 is a much more dangerous than its non-technological version. Indeed, in an Internet-based world: 1) it takes considerably less efforts to generate initial or sustained contacts between the agent and the target, 2) it takes considerably less effort to generate compromising material, and finally 3) consequences of blackmail can be made public considerably more easily with devastating effects on the victim's private life.

Sadly enough, examples of the impact of online sexually based blackmail threats can easily be found. On the beginning of November 2018, Ontario conservative MP Tony Clement had to resign Commons duties following what he claimed to be an extortion attempt after having shared sexually explicit images and video with an individual online (Tasker & Kapelos, 2018). In a statement made to the media, Tony Clement summarized the situation pretty well:

> "*Over the last three weeks, I have shared sexually explicit images and a video of myself to someone who I believed was a consenting female recipient. The recipient was, in fact, an individual or party who targeted me for the purpose of financial extortion.*" (Tasker & Kapelos, 2018)

This few sentences describe perfectly what a general *modus operandi* for such attack could be. Yet, what could have been a relatively classical extortion scandal was made more problematic by the functions occupied by Tony Clement. Indeed, Clement was acting as the Canadian conservatory party's justice critic

in the House – a role which was giving him access to critical information. Even worse in terms of security, he was serving on a number of parliamentary and other governing committees – particularly a high operative, recently created national security and intelligence committee (Tasker, 2018).

This case study posits several important questions. One of them is related to the problem of information access and security clearance in the digital age. The specific and privileged access that selected (usually elected) people have to critical, national security, or otherwise classified information has always existed. This access is an essential element of control of public action – transparency is a key principle for the good functioning of democratic societies. As a parliamentary member of a committee reviewing the work of Canada's intelligence agencies, Clement had notably access to the work of the Canadian Security Intelligence Service, to the Royal Canadian Mounted Police, the Canada Border Services Agency, and the Communications Security Establishment (Government of Canada, 2017; Tasker, 2018). The evolution of technologies does not change the rationale nor the relevance of this access of some individuals to information, rather it modifies the access to these individuals by others. Online presence makes people who are depositary of critical information considerably more accessible than they used to be. Two parameters characterize this increased accessibility of these potential targets. First, the size of the social circle (i.e., the number of people who have a direct contact with the target) is of a fully different magnitude with social media than if relying only on conventional contacts. Second, in order to have access to the target in conventional settings, people need to pass through several social filters. This is obviously much less the case with online media. Thus, technology changes the nature of the access to individuals both quantitatively (more people can access a given person) and qualitatively (there is less control on who can access a given person). In this context, by facilitating online contacts, sexually motivated online behavior tends to lower even more the threshold of entry of the social network of the target, thus giving the opportunity to gain leverage against the information holders. Tony Clement had to face political – and personal – consequences because his behavior was publicly exposed by the media. But what if this was not revealed? That is the very principle of blackmailing. Yet, social media exacerbate the magnitude of potential revelations, and consequently their impacts on one's career and private life. More than ever before, some might consider these consequences too high of a price, and may thus succumb to the easiest way – complying to the demands of the blackmailers. In this context, counter-intelligence services have to deal with the challenges related to this new reality of social media profoundly impacting the levels of public trust toward elected representative and other government officials.

Online dating applications

Online dating sites and applications have considerably modified the way romantic encounters can happen. They have also drastically increased the risks of being the target of sexually based online manipulations. Compared to conventional blackmailing strategies, online dating applications open fully new avenues for potential security breaches. Indeed, blackmailing is usually an active process from the point of view of criminal agents. They have to actively elicit situations for their target to meet with the fake romantic encounter in order for the bait to work. In contrast, individuals willingly joining online dating applications with the exact aim of finding romantic partners. From a manipulation perspective, it is not anymore the agent who moves toward the target, but the potential target who put itself right on display.

The level of self-vigilance on such application is definitively low, and a relation does not need to become intimate to trigger online contacts, as evidenced by hints from the dating industry. For instance, ads from the dating company "It's just lunch" mentions that "1.5X men are more likely to "friend" someone within 1 week after a first date and ¾ of people like to receive a texto after a "good" date." Once a cybercontact is made, the security of the whole network gets compromised. Indeed, intrusions in the social network of an individual gives access to a considerable amount of personal information – what could be referred to as social spying. While people will tend to keep different privacy levels between their professional network and their "friends" on social media, agents might be able to access this intimate circle through online dating applications. Another issue is that people tend to consult online dating application in public places such as coffee shops or train stations. Obviously, such public networks are not secured and could be easily targeted by cybercriminals of all sorts. Would the connections be made by the same device that would be used to work – which is likely to be the case – the professional network might potentially get compromised in its totality.

Relations starting through online dating applications can go further than chat flirting. With exchanges of sexually explicit material or real life encounters, situations can evolve to become similar to blackmail. However, the consequences for the individual are much worse. Indeed, in contrast to blackmail where the person was specifically targeted to "fall" into a trap, joining an online dating site or using an online dating application is a choice made freely and consciously by the individual. Thus, it becomes very difficult for the individual to claim any status of victim for the public eyes. It is important to note that being in a relationship does not seem to be an obstacle for online dating applications users. For instance, almost one Tinder's user on four is in a committed relationship while on the app (Timmermans, De Caluwé, & Alexopoulos, 2018).

Compromising someone using online dating applications is a bit different in terms of strategy than for conventional blackmail. In the case of blackmailing, the

difficulty is to make the target act in a compromising way. In the case of online dating applications, the goal is not to have the target act, but to be able to identify and locate the target within the crowd of users of the application. While this might at a first glance sound quite challenging, it is in fact not that complicated, especially with applications using geologicalizing features (for instance, Happn, an app that point the location where you crossed paths with another member). A putative scenario would go as follow: running such an application in the vicinity of any sensible building would allow to immediately identify all workers active on the application network. From there, it would be easy for an agent to select the right target from already visual identification through the profile pictures, and to trigger online contact, and if needed, offline contacts. Although such scenario may seem purely hypothetical, it easiness of implementation emphases the risks associated with online dating applications.

Online pornography

The rise of the Internet has considerably enhanced the landscape of pornography production and consumption. Over the last decades, online spaces have made pornography material widely accessible, transforming what was once a niche behavior into a wide-spread consuming behavior (Guitton, 2019a). Consequently, consuming online pornography is nowadays considered as a normative behavior by many people (Price, Patterson, Regnerus, & Walley, 2016). Because of its growing social acceptance, online pornography is not perceived as a source of security threat by the overwhelming majority of the population. However, consumption of online pornography is not a neutral activity when it comes to potential cyberthreats.

Widespread online pornography consumption is still a relatively recent phenomenon, and people behavior has yet to adapt to the new reality of cybersecurity. Indeed, it appears that some actions are not perceived as putting threats – even in physical settings, which are supposed to be highly secured. Protection against threats related to online pornography is surprisingly weak, including in locations that one would consider the most sacred centers of power. For example, official data released following a freedom of information request made by the Press Association revealed breathtaking volumes of connections to online pornography resources directly from the computer network of the House of Lords and the House of Commons – the two chambers of the British parliament (Press Association, 2018). Only between June and October 2017, well above 24,000 attempts were made from the parliamentary network – i.e., computers and connected devices specifically used by MPs and parliamentary staff (Press Association, 2018). These numbers are considerable: the average of 160 requests of connection to online pornography per day represents as many opportunities for security breaches.

Cyberthreats related to online pornography are mostly associated to behavior related to browsing activities. Despite the existence of paying sites, the vast majority of the online pornography landscape is made by aggregators of pornographic material. Viewing material through these aggregating platforms is free, but triggers massive exposure to various ads – this represents a simple yet powerful business model. The ads can take various forms, ranging from clickable links to pop-up windows. These "side" stimuli increase the odds of security break, by clicking and activating scripts which could represent potential threats. In this case, "side" can be understood in all its meaning, given that the ads and other commercial links are actually typically found on the screen on the side of the main (and usually central) window of the online video player. Once the script is launched, the system is potentially corrupted. While people are usually well aware of the risks related to fraudulent email and other phishing attempts, they are however typically much less alerted to the risks inherent to browsing activities. Taking again the example of the British parliament, believing that the connections to online pornography made from this venerable institution are mostly accidental – as suggested by the Parliamentary authorities (Press Association, 2018) – is a bit naive. Obviously, a majority of them are intentional. This accidental vs. intentional nature of the connection does have an impact in terms of cybersecurity. Indeed, if clicks can occur in any case, the probability to have clicks in an intentional browsing process is considerably higher than if the process is purely accidental. Thus, online pornography literally represents a potential Trojan horse, an open door for malwares and spying software.

As the technology itself, online behaviors are constantly evolving. One of the recent observed trends is the gamification of virtual spaces, i.e., the increase of popularity, availability (both in terms of number and of accessibility of the interfaces), and use of online games. Online adult games find a natural place on the continuum of online pornography: in fact, the only difference when compared to online video pornography viewing is an increase of the degree of interactivity of the material. In terms of cybersecurity, this new format bears at least two categories of risks. First, and quite obviously, online games require actions in order to be played – either installing elements on the computer or simply clicking the commands embedded within the game interface. This is an explicit and direct increase of the risks that were already mentioned above. Second, playing an online game means creating a history of play, so that the player can progress in the game. This can take different forms depending on the game mechanics, including level ups of the player's character, access to new levels/areas within the game metaverse – which would mean in the context of an adult game access to more adult material. This history creates game-related data, which are linked to data related to the game character (the "avatar"). Yet, these data are often as well linked, at least partially, to the player himself. This is, for instance, the case if the game offers some options accessible only after

payment, or when, due to the nature of the material presented in the game, age verification is required. These issues are not typical of online adult game. Some of these challenges – both ethic or related to data privacy and security break – have been already documented for online health games (Guitton, 2015). If such challenges exist for online health games – games which are much more controlled and have by definition a genuine goal – it is quite obvious that they will also be present, only exacerbated, in the context of online adult games.

Finally, when it comes to cybersecurity, a major issue of online pornography compared to other sexual behavior-based threats is that this form of danger can be fully automated. In other words, spying strategies based on online pornography browsing does not involve having identifiable individuals entering into contact with the target. As a direct consequence, trying to identify the aggressor based on specific contacts made with the target, or even just through data aggregation strategies (of digital footprints, activity patterns, etc.) is rendered simply irrelevant, making detecting or countering the threat quite challenging.

Identifying the targets

Although any individual holding relevant information could potentially be the target of information gathering attempts, victims of sexually based online manipulations in an intelligence context are typically drawn from a few specific populations. We will explore in the following paragraphs some of these populations, and describe their characteristic when it comes to cyberbehavior.

Students

In February 2018, FBI Director Christopher Wray mentioned the increase of non-conventional strategies of intelligence, specifically those targeting scientists, professors, and students. With well above 300,000 Chinese students in the USA per year, China was clearly a source of concerns for US officials – so much that some of the advisors of President Trump suggested for a time a US ban on student visas for Chinese students (Sevastopulo & Mitchell, 2018). This perception of foreign students as potential security threat is not specific to American paranoia: China regularly charges Taiwan to use students to spy upon its national affairs. Stories of young Chinese students entertaining romantic or sexual encounters with Taiwanese spies and consequently betraying their country appear regularly in China official media. Interestingly, while money was classically considered as the main rationale for betrayal, the terms “love,” “seduction,” and “Internet” appear more and more together in media such as China Central TV (CCTV). This choice of

words in the context of Chinese official media should not be considered neutral or purely rhetorical.

Although it is difficult to decipher the relative weight of reality vs. irrational fears and propaganda, the increase of student international mobility is considerable, exponential, and continuous. Thus, this problematic is becoming global. From a pragmatic point of view, the numbers and proportions of international students present in any campus are going to rise. Despite the recurrent tensions between mainland China and Taiwan, more than 10,500 Taiwanese students went to study in China in 2015. Although one would think that targets would be found a priori within graduate cohorts (Master or Doctoral students) enrolled in curriculums where exposure to strategic information could happen (e.g., military sciences, technology, politics, economics), any field, from molecular biology and toxicology to humanities or journalism could be of interest for foreign intelligence services. Trying to eradicate spying by forbidding foreign student to join national universities would not only be counter-productive, it simply is unrealistic. Of note, this phenomenon is not anymore limited to large research-intensive campus but also occurs on less prestigious universities or and smaller campuses – institutions in which professors and administrators might be less aware of the challenges and issues related to industrial/academic spying.

In terms of intelligence approaches based upon online sexual manipulations, students do represent a vulnerable population. As young and inexperienced adults typically cut from their immediate family context, students represent an easy target for sexually oriented strategies. Since students will evolve into professional life once they are done studying, the leaders of tomorrow are to be found among the best students. Thus, targeting students may represent a long-term investment for intelligence services: targeting individuals with romantic-based strategies when they are early stage students is easier than targeting them at later stage of their professional career. In this view, online spaces represent powerful tools. With Internet technologies and social media, romantic relationships do not have to be strictly physical anymore. Furthermore, online communication technologies allow distance relationships to survive much easier than before, thus making the time window of vulnerability much larger. Real life encounters initially limited in time can become long-lasting relationship easier – the intelligence agent being able to stay in safety in the original country, protected and unreachable by counter-intelligence services of the country of the targeted student.

It is important to note here that generational gap does not occur immediately when students leave university to enter professional life. Junior workers have offline and online behaviors very similar, not to say identical, to those of students. This is especially true for workers in the field of new technologies, including workers in companies bearing critical importance for intelligence services – or for that matter, intelligence and counterintelligence

technology workers themselves. Such online behaviors would include among others a heavy use of Internet, important presence on social media, and high degree of online connectivity. Therefore, everything that has been said for students could mostly be applied to young adults as well.

(Mature) Men

Popular representations of the relation between sex and spying will inevitably depict visions of men in situation of power being the main target of sexual blackmail. This category obviously includes politicians, who seem to be prominently represented in the news. This category also includes businessmen, high-level military officials, and – in a world were knowledge is more and more a synonym of economical competitiveness – potentially high-level researchers. In an age of media powered by social media and the Internet, sexual blackmailing of mature men represents a powerful leverage. Indeed, thanks to social media and the Internet, the public disclosure of such affairs does not even need the intervention of conventional media anymore. Thus, the impact on their career and on their family lives can be clearly devastating. The most mature the individual is, the more likely the person would be to have well-developed families (wife and children), increasing even more the negative impact of public revelation of potential affair or non-conventional sexual practices.

Numerous websites are targeting men through presentation of profiles of highly attractive young women (often displaying retouched pictures) accompanied by explicit slogans. A vast number of these sites use ethnicity as a "sale argument" – sites promising the male users to meet "Russian/Slavic Girls", "Asian Girls", and so on (Figure 1). Even more interesting, numerous sites are specifically and explicitly targeting older men through profiles of younger women. It is of course not criminal per se for a man to be attracted by younger women. Yet, it is obviously unrealistic for hundreds or thousands of attractive young women to be willing to consider only much older men as romantic partners. The lure, however, is quite efficient, as evidenced by the amount of website using this strategy to attract male customers (Figure 1). Finally, a specific niche is even more problematic: dating sites proposing "secret" relationships for married men. These extra-marital sites, often using a "sugar daddy" rhetoric (and might be perceived as bordering legality), offer a particularly convenient vehicle for intelligence-related seduction attempts. The resignation in December 2018 of the Australian MP Andrew Broad, Assistant Minister to the Deputy Prime Minister after a 'sugar daddy' sex scandal is a good example of how easy it is for men in position of authority to fall due to inappropriate online sexual behavior (Chung, 2018). The vulnerability of men to such temptation should not be underestimated, and no factor, including religiosity (Baltazar et al., 2010) or relationship status

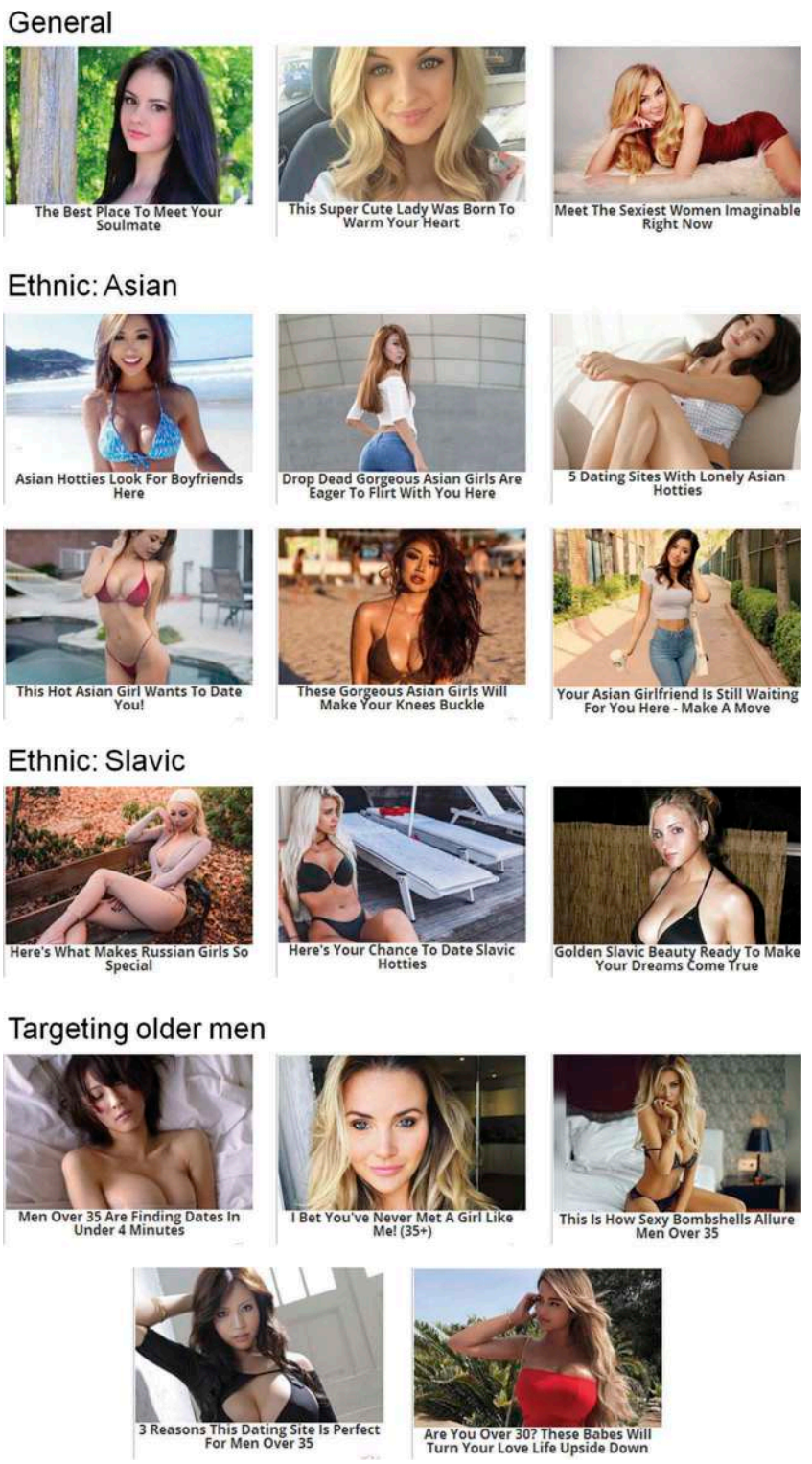

Figure 1. Examples of adds for online dating sites targeting men. Example of online adds for dating sites. Adds were sorted according to the rhetoric of the text: general (upper line), ethnic: Asian (second and third lines from the top), ethnic: Slavic (fourth line from the top), and finally, or targeting specifically older men (two last lines from the top). Please note the narrative associated with each picture.

(Timmermans et al., 2018), appears to be sufficient to prevent this vulnerability. Furthermore, some factors can increase this vulnerability. For instance, individuals presenting high degree of narcissism are more susceptible to fall for phishing attacks (Curtis, Rajivan, Jones, & Cleotilde Gonzalez, 2018) – of note, a personality trait, which may easily get reinforced in situation of power.

We will not extend much further the analysis of this specific category of targets. Still, a last factor is worth mentioning: currently, mature men are not digital native. In other words, they did not grow up with Internet technology and had to adjust their behavior at a latter stage of their life. Consequently, they are less familiar with dealing with the risks related to information technologies than would be younger individuals. This situation will progressively evolves as time passes, yet it will take a few more decades for the digital natives to occupy the upper niches of executive seniority and decisional power.

(Young) Women

International terrorism organizations such as ISIS heavily rely on the influx of foreigners (usually from the Western countries) to grow their ranks. Since, for obvious reasons, direct in-person recruitment is typically out-of-order, this kind of organization tends to make a heavy use of online media to reach potential new recruits. However, it is quite interesting to see that the strategies that will be used are very different depending on the target, i.e., to recruit men or to recruit women. Strategies to recruit men into this kind of organization through online spaces rely on a modern avatar of propaganda. Potential recruits are baited using rhetoric and imagery based on a mix of violent messages (typically centered around para-military tropes) and communitarian elements (often also depicting violence, abuses, or injustices that the community is experiencing or suggested to experience). Those messages are propagated by social networks – initially, limited version circulates through the main social media, and as the messages get more and more explicit, through specialized forums closer and closer to the Dark Net. The imagery and rhetoric is deliberately designed and produced to appeal to an idealized version of the fight – the terrorists are not depicted as heartless murderers, but as people displaying manly (even heroic) values, and are propelled to a status of role-models for the potential recruits. These strategies are basically the same than conventional offline strategies used since more than a century – the main (if not only) differences being the magnitude of the phenomenon when using online spaces and the increased difficulties to locate, monitor, control, or arrest the potential recruiters.

The situation is quite different when it comes to women. Indeed, the strategies used by terrorism organizations in the case of women will be

mostly based on seduction – which brings us back in the main scope of this analysis, Online romance will be the main vector used by such organizations to recruit females within their ranks, Male agents, often located outside of the living area/country of the women, will establish initial online contact using various – typically humanitarian or communitarian – excuses. The agent will then progressively lure the woman into a romantic relationship. Although involving cognitive and socio-affective processes slightly different than for offline intimacy, online intimacy can clearly produce an attachment as strong as real-life contacts would (Lomanowska & Guitton, 2016). A few decades of research in eMarketing taught us that using emotions is probably the best way to convince an online viewer. While pre-existing attitudes are obviously important in the way viewers are influenced by ideological websites, this influence can be deeply modulated by emotional appeal (the reader interested by this topic is referred to the excellent experimental study by Ness et al., 2017, which analyzed the impact of manipulating emotional appeal and valence of an ideological website on the attitude of the viewers). And is there a stronger emotion than love? Progressively, the target will alter her offline behavior, and if the recruiting attempt is successful, is likely to leave her country to meet her love interest. In terms of social network dynamics, men targeted by terrorist organizations have a diffuse network, made of several small nucleus or nodes of people, In contrast, women targeted by the same organizations will typically have a single interlocutor: their love interest.

Obviously, attempts of Internet-based criminal manipulations (such as phishing or identity usurpation) can target women of any age. However, the focus of this analysis is on sexually oriented behavior in an intelligence context. In this view, online sexually based manipulations tend to target younger over mature females. In the context of the utilization of sexual behavior as a manipulative tool, a two-folds gendered dichotomy is thus appearing: men and women differ both in terms of the age of the target and of the purpose of targeting. Beside students, targeted men will mostly be mature, and targeted for intelligence (information gathering) purposes, while women will be mostly younger, and typically targeted for terrorism recruitment purposes.

Counterintelligence and protection strategies

"I recognize now that I have gone down a wrong path and have exercised very poor judgment," said Tony Clement in a public statement after his online misbehaviors were exposed (Tasker & Kapelos, 2018). Although Clement's scandal led to an investigation by the Canada national security agencies to determine if critical information were compromised (Tasker, 2018), this situation should not have happened in the first place if

appropriate cyberbehavior would have been adopted by Clement. Although practicing common sense and exercising good judgment should be the first and foremost defense against cybercriminality, we can not anymore rely solely on these basic means. Indeed, given what Human nature is, it would be utopic to consider that goodwill alone is enough to avoid these dangers. If categorization and model-building can be performed to sort the different cyberthreats and the potential targets – what we have attempted to do so far – the same strategies can unfortunately not apply under the same form for developing counterintelligence measures. Indeed, online behaviors are highly multi-dimensional. Thus, strategies of cyber-counterintelligence cannot strictly overlap the taxonomy of threats. Furthermore, given that the aim of counterintelligence is to protect information, protection strategies should be mostly directed toward the potential targets of information thievery, i.e., people not necessarily related to the intelligence community, but having access to sensitive information. Specific actions can be taken to develop appropriate countermeasures against the cyberthreats related to online sexual behaviors – whatever the exact nature of the threat. We will be hinting here about some actions that could be developed. Of note, these potential actions are not directly related to increasing security protocols. Overall, three categories of measures can be implemented: 1) non-specific measures related to cybersecurity, 2) specific measures at the organizational level targeting individuals, and 3) specific measures at the government/structural level. The following paragraphs will list a few of possible measures – they are by no means the only ones which could be implemented.

Non-specific measures

- *Promoting healthy online life habits*. The first set of countermeasures represents solutions that are common to any cyberthreats and relates to how to live safely in virtual spaces and in a heavily digitalized world. More than others, people having access to potentially critical information should keep a high level of vigilance throughout all online activities, including in personal settings. Even without doing any illicit operation when using computers and connected devices, there are always risks to get infected by malware. Basic measures aiming at keeping healthy online life include avoiding clicking on attached files or hyperlink from unknown sources, avoiding consulting suspicious Websites, avoiding to work on or transmit critical data when on a public network, or being otherwise careful not to put the computer network of the organization at risk by imprudent behaviors. Although this might be considered as common sense by digital native, it is not necessarily, and certainly not automatic for digital migrants – to whom still belong the vast majority of potential targets for a few more decades.

- *Raising awareness among potential targets*. If theoretically any individual can be the victim of sexually based blackmailing or of other forms of manipulation through online sexual behavior, practically, some people are more at risk than others. Raising awareness to cybersecurity issues has been demonstrated to have positive impact on security-related behavior (Mamonov & Benbunan-Fich, 2018). Some factors drastically increase the risks of be considered as a potential target in a context of foreign intelligence. Having access to critical information, having access to secured locations, having access to critical people – all these are elements that can make an individual worth being targeted through online sexual manipulation. These parameters are part of the functions and responsibilities associated with the professional activities of the potential target. Yet, people in such situation should not adopt online behaviors that could put them – and through them, the information they are holding – at risk. More than for other workers, people who might be at risk of being targeted for information gathering purposes should be made aware of the potential risks that could be associated with online sexual activities.
- *Reinforcing personal ethics*. An overwhelming proportion of people caught in scandals related to online sexual activities will claim to the media having lacking good judgment. Obviously, poor judgment is not always criminal. That being said, social media-powered scandals are typically arising from behavior that should not have occurred in the first place. More than just exercising good judgment, it could be advised to people in situation of power and other opinion leaders to reflect on their own personal ethical values. If not a moral stance, one should, at the very least adopt a pragmatic point of view: the consequences of a sexual scandal in the digital era can be devastating not only for oneself but also for family and friends.

Specific measures at the organizational level targeting individuals

- *Controlling the access to online adult websites and applications in sensitive physical sites*. Independently of any moral consideration, access to online pornography websites or online dating applications should be prohibited inside and in the vicinity of highly secured or critical locations. Obviously, online pornography sites should not be accessed in some buildings of national importance, but the British Parliament experience tells us they massively are. Although this is yet to be documented, the same is likely true for online dating applications. This would reduce the odds of being infected by Trojan horse types of viruses or malwares, and will make the efforts of foreign agencies to establish

contacts with workers through romantic and/or sexual encounters more difficult. With a growing understanding of problematic Internet use and online pornography addiction, psychological assessments might be used at some point to identify individual vulnerabilities and weaknesses. Although such approaches would be ethically questionable for regular companies, they might be justified in a context of people having access to sensitive information, alongside the other security checks made by counterintelligence services.

- *Limiting interconnection between private and working stations*. Users should avoid as much as possible unnecessary contacts between secured working stations and apparatus used to access online adult material. In this view, developing habits of using different apparatus for different tasks to avoid the risks of contaminations from one working station (whatever its nature) to another across online interfaces.
- *Offering support to individuals*. While all institutional or company-oriented training programs should include at least some degree of basic training in cybersecurity, security issues related to online sexual behaviors raises specific issues and difficulties. Companies or institutional organizations that could be the target of attempts of manipulation through online sexual behavior should adopt strategies to offer support to their workers (Furnell, Kern-am-nuai, Esmael, Yang, & Li, 2018). This could be done notably under the form of specific training (*in situ* (on-site) training, continuous training) or under the form of mentoring. In order to be able to reach properly vulnerable individuals, mentoring should optimally have to be organized by the hierarchy in a way that would keep a reasonable degree of anonymity to the individuals. In such settings, training in cybersecurity issues should include specific elements to deal with these aspects in a holistic perspective (and not just from a purely technical point of view).

Specific measures at the government/structural level

- *Developing specialized formations by higher learning public institutions*. All strategies taking place at the structural level take advantage of the capacity of governments to have an impact on educational systems. The first type of governmental counter-measures is to promote the development of formation in cybersecurity which would not focus solely on the technical/technological aspects (hardware and software, security protocols, encryption algorithms, etc.) but would encompass the dimensions of individual cyberbehavior. Typically, cybersecurity formations are aimed at IT professionals. This would not be the case anymore, as psychology and even humanities content would become a major part

of the cursus. Such formation could be developed and provided by universities and other higher learning institutions, or directly by the government agencies facing potential cybersecurity threats. Private companies fearing industrial piracy or working with critical data could also implement such kind of training, which could be accompanied by a certification of (cyber)security clearance. Although these formation could take the form of conventional courses, online courses under a MOOC model could also represent an interesting solution (of note, a search of any of the largest MOOC databases using cybersecurity as a keyword will mostly direct to formations related to the hardware/software aspects, typically with no mention to behavioral or Human factor aspects). Such kind of project of course development could be funded publicly as a part of a larger effort from a government to build a national workforce on cybersecurity.

- *Including problematic related to sexual cyberbehavior into other curriculums*. Beside the development of specialized cursus, courses dealing with the understanding of online sexual behavior could be included in formation not primarily aimed at cybersecurity. Numerous types of cursus could benefit from the inclusion of such topics in their curriculum, ranging from management and marketing to psychology and administration. Such a strategy would also favor a cross-fertilization both in terms of research and teaching in fields not typically associated with intelligence and counter-intelligence. The means that governments could use to support the inclusion of courses on sexual cyberbehavior in non-specialized formations could be either direct (by regulatory way, for example, by issuing policies forcing certain curriculums to include such courses in order to have the degree validated by national accreditation agencies) or indirect (for instance through the valorization of formation on such topics in recruitment profiles for state-controlled jobs) or by promoting otherwise universities adding such elements in their cursus). In this context, it is important to remember that in a lot of countries, most academic positions are public positions, offering the local government the power to define employment criterions.
- *Developing a specialized workshop*. Governments can take global measure to build and develop a specialized workforce within its population, which could provide internal expertise on issues related to online sexual behavior. Governments have a general view of their national workforce. Through the control of regulation, of public funds, of educational policies (including accessibility and accreditation of formations), governments can have a direct impact on the development of workforce in certain fields. In the context of online sexuality, some nations might already be engaged in a similar process to develop academic/scholarly workforce. As the Editor-in-Chief of "Computers in Human Behavior,"

one of the leading journals in the field of cyberpsychology, the author of the present study noticed that the number of submissions from Chinese scholars dealing with online pornography has significantly increased over the last few years, suggesting that some countries are indeed developing such specialized workforce in their academic environment. On a country-wide scale, this workforce does not have to be primarily military, nor even governmental. Civilian experts are perfectly fine, as long as enough of them are available to support intelligence or counter-intelligence services would the need arise. For a country, to have this kind of expertise spread across its academic ecosystem represents a potential strategic edge when it comes to national cybersecurity. Indeed, as even more students get exposed to these problematic, the global awareness of such issues among the future decision leaders of the country will only increase. Once such a workforce is built, it will be important to make sure to be able to identify properly this expertise, to identify properly the people having this expertise, and to insure their availability. Indeed, the relationships between the academic and intelligence worlds are historically complex, something which needs to be taken into account (Crosston, 2018). Increasing the quantity and availability of experts able to document, to analyze and to propose responses to online sexually based cyberthreats will also make it easier for this topic to be included in intelligence teaching curriculums.

Conclusion

Cyberpsychology is still an emerging discipline. The massive efforts put on large-scale cyberthreats should not occult the importance of individual behavior on other forms of menace, more insidious because less controllable. Individual weaknesses can not always be modeled; individual romantic encounters can not be planned. The question of the implications that the shift of sexuality to online spaces might have on national security and on personal development should be a source of concern. Without trying to do predictive science, there is nonetheless an interesting co-occurrence of elements suggesting that this might indeed already be the case in some countries.

Obviously, these phenomena are still poorly documented, paving the way for potentially irrational – or at the very least ineffective – responses from governments. In contrast to other forms of cyberthreats, manipulations based on online sexual behavior are depending on individual factors difficult to control – and might thus be more difficult to prevent. Because of this, this form of cyberthreat is potentially more dangerous than some others. Indeed, specific counter-measures are mostly behavioral in nature rather than associated with technological developments, creating vulnerability related to Human factor rather than to technology itself. Thus, first-line counter-

measures can only be behavioral as well, with education and training. As often in such situations, research will be the key to develop adapted and efficient solutions.

Although the media regularly put under the light online sex scandals involving high profile leaders, intelligence services worldwide seem to focus their attention and efforts on large-scale cyber-attacks. Machine-centered approaches, big data, and artificial intelligence are all tools with an extremely powerful potential. They will without doubt prove invaluable to the intelligence community. Yet, they are still just tools. We should always remember that what makes things operate at the end is the Human factor – particularly in the context of intelligence and information gathering. The impact of online sexuality on human behavior is a perfect example of that.

Disclosure statement

There is no conflict of interest associated with this work.

Funding

No funding reported for this work.

Notes on contributor

Matthieu J. Guitton is Full Professor and Secretary of the Faculty of Medicine at Université Laval (Quebec City, QC, Canada). He is Senior Researcher/Group Leader at the CERVO Brain Research Center (Quebec City, QC, Canada). A graduate from the University of Rouen and Université Pierre et Marie Curie – Paris VI, he obtained a PhD from the University of Montpellier (France) and was a Koshland Scholar - Postdoctoral Fellow of Excellence at the Weizmann Institute of Science (Rehovot, Israel). He is a Fellow of the Royal Anthropological Institute. He is the Editor-in-Chief of Computers in Human Behavior and serves on several other editorial boards, such as Current Opinion in Behavioral Sciences. He is an expert in cyberpsychology and cyberbehavior.

References

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quartely*, *34*(3), 613–643. doi:10.2307/25750694

Baltazar, A., Helm, H. W., Jr, McBride, D., Hopkins, G., & Stevens, J. V., Jr. (2010). Internet pornography use in the context of external and internal religiosity. *Journal of Psychology and Theology*, *38*(1), 32–40. doi:10.1177/009164711003800103

Bindu, P. V., Santhi Thilagam, P., & Ahuja, D. (2017). Discovering suspicious behavior in multilayer social networks. *Computers in Human Behavior*, *73*, 568–682. doi:10.1016/j.chb.2017.04.001

Bower, D. E. (1990). *Sex espionage*. New York, NY: Knightsbridge.

Chung, F. (2018). 'It speaks to the climate of women': Sugar baby website says Andrew Broad was a #MeToo casualty. *news.com.au*. Retrieved from https://www.news.com.au/finance/work/leaders/it-speaks-to-the-climate-of-women-sugar-baby-website-says-andrew-broad-was-a-metoo-casualty/news-story/7e8236368f8e9deec2aa23e0eec3a72f

Crosston, M. D. (2018). Fragile friendships: Partnerships between the academy and intelligence. *International Journal of Intelligence and CounterIntelligence*, *31*(1), 139–158. doi:10.1080/08850607.2017.1337448

Curtis, S. R., Rajivan, P., Jones, D. N., & Cleotilde Gonzalez, C. (2018). Phishing attempts among the dark triad: Patterns of attack and vulnerability. *Computers in Human Behavior*, *87*, 174–182. doi:10.1016/j.chb.2018.05.037

Fife, R. (2018). Canada arrests Huawei's global chief financial officer in Vancouver. *The Globe and Mail*. Retrieved from https://www.theglobeandmail.com/canada/article-canada-has-arrested-huaweis-global-chief-financial-officer-in/

Furnell, S., Kern-am-nuai, W., Esmael, R., Yang, W., & Li, N. (2018). Enhancing security behaviour by supporting the user. *Computers & Security*, *75*, 1–9. doi:10.1016/j.cose.2018.01.016

Government of Canada. (2017). Retrieved from https://pm.gc.ca/eng/news/2017/11/06/prime-minister-announces-new-national-security-and-intelligence-committee

Guitton, M. J. (2011). Immersive role of non-required social actions in virtual settings: The example of trade role-play in the second life Gorean community. *Design Principles and Practices: an International Journal*, *5*(1), 209–220. doi:10.18848/1833-1874/CGP/v05i01/38012

Guitton, M. J. (2012). Living in the hutt space: Immersive process in the Star Wars role-play community of second life. *Computers in Human Behavior*, *28*(5), 1681–1691. doi:10.1016/j.chb.2012.04.006

Guitton, M. J. (2015). Ethical challenges in online health games. In D. Novák, B. Tulu, & H. Brendryen (Eds.), *Handbook of research on holistic perspectives in gamification for clinical practice* (pp. 1–9). Hershey, USA: IGI Global.

Guitton, M. J. (2019a). Mitigation of health risks in consensual non conventional sexual pratices: Could cyberspace provide new solution? *Computers in Human Behavior*, *91*, 346–347. doi:10.1016/j.chb.2018.04.010

Guitton, M. J. (2019b). Facing cyberthreats: Answering the new security challenges of the digital age. *Computers in Human Behavior*, *95*, 175–176. doi:10.1016/j.chb.2019.01.017

Lahneman, W. J. (2016). IC data mining in the post-snowden era. *International Journal of Intelligence and CounterIntelligence*, *29*(4), 700–723. doi:10.1080/08850607.2016.1148488

Lewis, D. (1976). *Sexpionage: The exploitation of sex by soviet intelligence*. New York, NY: Harcourt Brace Jovanovich.

Lomanowska, A. M., & Guitton, M. J. (2016). Online intimacy and well-being in the digital age. *Internet Interventions*, *4*(2), 138–144. doi:10.1016/j.invent.2016.06.005

Lord, J. (2015). Undercover under threat: Cover identity, clandestine activity, and covert action in the digital age. *International Journal of Intelligence and CounterIntelligence*, *28*(4), 666–691. doi:10.1080/08850607.2015.1022464

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32–44. doi:10.1016/j.chb.2018.01.028

Matz, S. C., Kosinski, M., Nave, G., & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences of the U.S.A.*, *114*(48), 12714–12719. doi:10.1073/pnas.1710966114

McCole, P., Ramsey, E., & Williams, J. (2010). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research*, *63*(9–10), 1018–1024. doi:10.1016/j.jbusres.2009.02.025

Ness, A. M., Johnson, G., Ault, M. K., Taylor, W. D., Griffith, J. A., Connelly, S., … Jensen, M. L. (2017). Reactions to ideological websites: The impact of emotional appeals, credibility, and pre-existing attitudes. *Computers in Human Behavior*, *72*, 496–511. doi:10.1016/j.chb.2017.02.061

Park, C. H., & Kim, Y. G. (2003). Identifying key factors affecting consumer purchase behavior in an online shopping context. *International Journal of Retail & Distribution Management*, *31*(1), 16–29. doi:10.1108/09590550310457818

Press Association. (2018). Parliament reports 24,000 attempts to access pornographic websites since election. *The Guardian*. Retrieved from https://www.theguardian.com/politics/2018/jan/08/parliament-reports-24000-attempts-to-access-pornographic-websites-since-election

Price, J., Patterson, R., Regnerus, M., & Walley, J. (2016). How much more xxx is generation x consuming? Evidence of changing attitudes and behaviors related to pornography since 1973. *Journal of Sex Research*, *53*(1), 12–20. doi:10.1080/00224499.2014.1003773

Ratnasingham, P. (1998). The importance of trust in electronic commerce. *Internet Research*, *8*(4), 313–321. doi:10.1108/10662249810231050

Saramäki, J., Leicht, E. A., López, E., Roberts, S. G. B., Reed-Tsochas, F., & Dunbar, R. I. M. (2014). Persistence of social signatures in human communication. *Proceedings of the National Academy of Sciences of the U.S.A.*, *111*(3), 942–947. doi:10.1073/pnas.1308540110

Sevastopulo, D., & Mitchell, T. (2018). US considered ban on student visas for Chinese nationals. *The Financial Times*. Retrieved from https://www.ft.com/content/fc413158-c5f1-11e8-82bf-ab93d0a9b321

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behavior. *Computers & Security*, *24*(2), 124–133. doi:10.1016/j.cose.2004.07.001

Stewart, H. (2017). Damian Green sacked as first secretary of state after porn allegations. *The Guardian*. Retrieved from https://www.theguardian.com/politics/2017/dec/20/damian-green-resigns-as-first-secretary-of-state-after-porn-allegations

Tasker, J. P. (2018). Scheer asks Tony Clement to leave conservative caucus over sexting scandal. *CBC News*. Retrieved from https://www.cbc.ca/news/politics/clement-scheer-explicit-photos-1.4895295

Tasker, J. P., & Kapelos, V. (2018). Conservative MP Tony Clement resigns commons duties over sexting scandal. *CBC News*. Retrieved from https://www.cbc.ca/news/politics/tony-clement-sexting-1.4894889

Taylor, T. L. (2002). Living digitally: Embodiment in virtual worlds. In R. Schroeder (Ed.), *The social life of avatars: Presence and interaction in shared virtual environments* (pp. 40–62). London, UK: Springer.

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376–391. doi:10.1016/j.cose.2017.07.003

Timmermans, E., De Caluwé, E., & Alexopoulos, C. (2018). Why are you cheating on tinder? Exploring users' motives and (dark) personality traits. *Computers in Human Behavior*, *89*, 129–139. doi:10.1016/j.chb.2018.07.040

van Schaik, P., Jeske, D., Onibokun, J., Conventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547–559. doi:10.1016/j.chb.2017.05.038