The "Strategic Corporal": Facing the Cyber Threat in French Armies and Homeland Security Forces

Antoine-Louis de Prémonville (officer in the French Army and independent researcher in History and Geopolitics)

Key Words: French Armies, homeland security, cyber threat, social networks, e-reputation, compromising, strategic corporal.

Introduction

The young men and women joining the ranks of the French Army and homeland security forces every year have a lot in common with their fellow citizens. Their habits, leisure, and tastes are those promoted in the everyday life. Contrary to the cliché, French servicemen don't live on the fringes of society. Most of them surf the Web and use social networks to keep in touch with their family and relatives while serving in France or overseas. In fact, nothing in particular seems to protect them against exterior threats; on the contrary, their activities make them valuable targets. Indeed, the French Armies and other security services have tended to adopt the newest trends and technologies for communication and self-promotion. Nowadays, the internet is available in every boot camp and most officers daily send e-mails daily for internal communication.

Granted by the French constitution, servicemen have the same rights as any other citizens —even if they obtained the right to vote after women, on August 17, 1945! However, among the very specificities of the military, they have a duty to exercise restraint regarding political, philosophical, and religious opinions, in order not to harm the e-reputation of the Armies.

As the very last wardens of the Republic, the armed forces should not allow servicemen to express personal points of view in the name of the institution. The dangers of this are clear. For example, even though some service members served loyally as members of Parliament under the Third Republic, the government at the time feared the influence of conservative officers, most of them Catholic, Bonapartist, or royalist. That is the reason why an 1875 law disqualified

them from standing as candidates for parliament election. Admittedly, Field Marshal de Mac Mahon openly endorsed plans for royalist restoration and General Boulanger had planned a military coup. Loyal but openly reluctant in his support for the republic, Field Marshal Lyautey was far too critical as a secretary of war. And, of course, we cannot forget Field Marshal Pétain and the Vichy regime.

Yet, today, expressing discord with the official line seems inconceivable. Recall that the army's nickname is the "Big Mute" (*la Grande Muette*)! Even if servicemen can be elected to Parliament, they must leave office for the duration of their term.[1] Along with the preservation of the reputation of the armed forces, the discretion of servicemen on social networks is thus a professional imperative.

In order not to compromise both the confidentiality of operations and their own security in a context of frequent terrorist attacks against representative of the state, servicemen must obviously keep some secrecy regarding their own engagement. It is not only an elementary professional skill; it is a primary need, for the consequences are often serious. Here, I will talk examine how servicemen's lack of discretion on social networks could harm the entire security organization. (1) First, I will discuss the e-reputational damage. (2) Then, I will focus on the risk of compromising missions, which is a threat that sometimes leads to (3) tragic and deadly endings.

Reputational Harm

In a famous article published in 1999, U.S.M.C. general Charles C. Krulak insisted on the role of "strategic corporals" in modern wars, that is to say, in asymmetric conflicts mixing peacekeeping and humanitarian aid in an over-mediatised atmosphere. His aim was to demonstrate that a low-rank private could seriously compromise the mission—and the

[1] "Laetitia Saint-Paul, seule militaire élue députée, fait son entrée à l'Assemblée," *Europe 1,* June 24, 2017, https://www.europe1.fr/politique/laetitia-saint-paul-seule-militaire-elue-deputee-fait-son-entree-a-lassemblee-nationale-3370739.

campaign as a whole—if a wrong decision with negative consequences were to be mediatised.[2] Subsequently, French retired colonel and academic Michel Goya tried to propose a mathematical formula for Krulak's concept. Namely, he wrote, "We could formulate an equation of the strategic corporal with the following elements:

- F representing the initial folly

- R representing the portrayal of the folly

- S representing its spreading in the media

- C representing the unfavourable context.

Note that C resonates with F. Indeed, an unfavourable context leads to folly, either deliberately because of provocative actions or simply due to an atmosphere of distrust."[3]

In April 2004, human rights violations committed by US Army and CIA personnel against detainees in the Abu Ghraib prison in Iraq came to public attention. The scandal tarnished the reputation of the US Army, whose mission was supposed to promote democracy and human rights. Condemned both within the United States and abroad, the affair is a textbook case of the strategic corporal's negative effect in cases of misconduct. Indeed, the infamous photos have remained visible on the Web, years after the prosecution and condemnation of black sheep servicemen.

Devastating for the reputation of the armed forces, dubious video with dead or submissive persons rapidly go viral because of the easy sharing on websites like YouTube. Similarly harmful, explicit references to renegade political regimes made by individuals wearing a uniform generally force top officials to condemn them. Haunted by its painful history and extremely vigilant when it comes to ethical issues, the Bundeswher was shaken by a

[2] Charles C. Krulak, "The Strategic Corporal: Leadership in the Three Block War," *Marines Magazine*, January 1999.

[3] Michel Goya, "Le caporal stratégique ou peut-on confiner la connerie?" *La Voie de l'épée*, June 1, 2020, https://lavoiedelepee.blogspot.com/2020/06/le-caporal-strategique-ou-peut-on.html.

"desecration of skulls" scandal in 2006.[4] In the same vein, German, Australian, or French armies—among others—have been confronted with leaked photos and videos showing servicemen praising the Third Reich.[5] However, praising horrors is not the only way for servicemen to tarnish the reputation of the institution they serve in. Numerous apparently "benign" cases underline how powerful and hurtful speeches and opinions by personnel may undermine the armed forces' image. For example, both the *gilets jaunes* ("yellow jackets") and the anti-gay marriage movements have been praised by an unknown number of members of the French Ministry of Defense. As individuals, they benefit from the liberty to demonstrate, provided they are dressed in civilian clothing. However, any incident or violence they are involved in during a demonstration is generally mentioned in the media, as is their membership in a public institution. Obviously, this does not mean that there are plenty of servicemen who belong to militant groups attacking the police and causing extensive damage. At the same time, during arrests of rioters and looters, some suspicious passers-by have been known to work for Defense. Even though they could be found innocent—black sheep do exist, let's not deny it—the career consequences are hardly ever neutral.[6]

There are other types of reputational risks besides servicemen holding objectionable opinions or taking part in violent riots. Between 2011 and 2016, the scandal over Louvois, the defective software dedicated to pay the wages of Army personnel, was directly responsible for massive unpaid wages, provoking delicate personal financial situations. In 2012 only, members

[4] Thomas Rid, "Les photos du caporal stratégique. Comment les nouveaux médias changent la guerre," IFRI, November 2006, https://www.ifri.org/en/publications/publications-ifri/articles-ifri/photos-caporal-strategique-medias-changent-guerre.

[5] "New Photos Link Elite German Soldiers to Nazi Emblem," *Deutsche Welle*, November 2, 2006, https://www.dw.com/en/new-photos-link-elite-german-soldiers-to-nazi-emblem/a-2223277; Dan Oakes, "Australian Soldiers Flew Nazi Swastika Flag from Vehicle in Afghanistan; PM Says Diggers' Actions 'Absolutely Wrong,'" *ABC*, June 13, 2018, https://www.abc.net.au/news/2018-06-14/photo-shows-nazi-flag-flown-over-australian-army-vehicle/9859618; "Trois militaires photographiés faisant le salut nazi," *Le Figaro*, April 2, 2008, https://www.lefigaro.fr/actualites/2008/04/02/01001-20080402ARTFIG00283-trois-militaires-photographies-faisant-le-salut-nazi.php.

[6] Jean-Dominique Merchet, "Une lettre du colonel Ruffier d'Epenoux," *L'Opinion*, June 18, 2013, https://www.lopinion.fr/blog/secret-defense/lettre-colonel-ruffier-d-epenoux-1164.

of the army experienced an estimated 465 million Euros in unpaid wages. While the Ministry of Defense did recognize the situation as a failure and acknowledged its shameful consequences, committees of servicemen spouses and partners popped up on social networks to denounce the unbearable circumstances into which they were thrust. The breaking of a kind of omertà suddenly enabled the media to address the consequences for families and the amount of public funds wasted in this dramatic failure.[7] Due to the outrage people expressed over the scandal, the Army had no choice but to jettison Louvois and replace it with a new software. For our purposes, even though the burden of responsibility rested with the politicians who had decided to implement the defective software, the scandal damaged the Army's reputation. Considering the slow political response and the hidden pressures some servicemen experienced from their hierarchy to silence some spousal committees, many soldiers, NCOs, officers, and their relatives did interpret the situation as a form of disrespect.

Compromising Missions

In addition to the risk of tarnishing the reputation of the Armed Forces, misuses of social network sites are very likely to compromise mission safety. What are we talking about, precisely? In any operation, one of the key success factors is keeping the highest possible level of confidentiality. When the enemy knows the very moment, the place, or the composition of the detachment, he is then capable to respond appropriately, adapting his own modes of action to foil ours. Indeed, knowing the enemy is essential to anticipating his modes of action. That is the reason why all Armed Forces have an intelligence service dedicated to the understanding of the enemy. However, the Armed Forces are not the only actors that try to adopt the opposite point of view.

The military capabilities of the enemies the French army has been fighting since the 2000s are inferior by far to French standards. However, it would be a serious mistake to consider these

[7] Jacques Monin, "Louvois, le logiciel qui a mis l'armée à Terre," *France Inter*, January 27, 2018.

terrorist armed groups as being unable to seek out information on our capabilities and modes of action. Certainly, their intelligence cells have limited means. Until we are shown proof to the contrary, the Islamic State or other Islamic armed groups in the Sahel lack high-tech intel capabilities such as satellites, electronic warfare, air support, or Special Forces operators. On the other hand, it would be risky to assume they are unimaginative. They have discernible capabilities of diverting certain technologies from their primary purpose or adapting obsolete military equipment to meet new needs. Those so-called barefoot thugs dressed in rags and driving rusty pickup trucks know how to design unpiloted armed aerial vehicles, send encrypted messages, and infiltrate government departments and agencies.

Considering their ability to inflict casualties and, what is more, to keep on fighting for years despite the limited means at their disposal and the tremendous losses experienced, we need to face that they have true professional skills. Moreover, maybe should we admit, too, that this enemy knows us better than we know him. Many terrorists were born and raised in Europe. Western pop culture influences anyone watching the television or listening to the radio anywhere in the world. That is the other side of soft power's double-edged sword. Hence, it would very be risky to underestimate the existing threat to the point where no safety precautions are taken. The ability to surf the Web and connect to social network sites is easily accessible worldwide. Moreover, accessing personal data nowadays is all the easier given that people share them with sometimes unknown third parties on the Web. Some people publicly share so many photos, videos, and posts on Facebook, Twitter, Instagram, YouTube, and so on, that one can easily establish a file on them. Unfortunately, some members of the armed forces (or any other public agency) misuse the online networks. Were an agent to forget that the Internet is not a forum for discussion about their missions but a means to stay in touch with relatives, he would compromise his mission. Such a situation is not hypothetical. One of the most famous cases happened in 2010, within the Israeli army. Specifically, an Israeli private published a post on

Facebook revealing details of an upcoming mission in the West Bank: "On Wednesday we are cleaning out the village of Katana (nr Ramallah) – today [an] arrest operation, tomorrow an arrest operation and then please god, home by Thursday." Other servicemen reported the post to the unit's commanding officer, who decided to cancel the mission for fear that operational security had been breached. In 2008 another Israeli soldier was jailed for uploading sensitive information onto Facebook.[8] Considering the number of social networks users in the French armed forces, such a possibility could arise there, too. A 2014 survey pointed out that three out of four army service members, most of them noncommissioned, were active social networks users. Only 11 percent had given up their online profiles [upon joining the army], whereas 15 percent (one out of three being officers) had never had any.[9] Hence, in 2012 the French Ministry of Defense released a *Guide to the Correct Use of Social Networks*. Meanwhile, cyber security experts regularly give conferences in boot camps and military academies to warn the personnel about the dangers posed by social networks to operations abroad and in the homeland.

More recently, new threats from social networks have arisen in the cyber battlefield. Deception is a well-known mode of operation aimed at influencing the enemy's manoeuvres. Now, it is being conducted on the Web. For example, some opponents of the French army in the Sahel spread obvious fake news to foster a popular anti-French movement. According to these fake news items, so-called friendly fires incidents by Barkhane operators would frequently involve its African allies. Others pretend that the French support armed terrorist groups. Clearly unfair and partisan, these lies are massively shared, "liked," and commented upon.[10]

[8] Simon McGregor-Wood, "Facebook Details Force Israeli Military to Cancel Operation," *ABC News*, March 4, 2010, https://abcnews.go.com/International/facebook-details-force-israeli-military-cancel-operation/story?id=10006343.

[9] Michel Sage, " Les militaires dans l'espace public numérique," in *Guerre, armées et communication*, ed. Eric Letouturier (Paris: CNRS éditions, 2019), 124.

[10] Laurent Lagneau, "Sahel: Sur les réseaux sociaux, la force Barkhane est visée par une campagne de fausses informations," *Opex360*, December 5, 2019, http://www.opex360.com/2019/12/05/sahel-sur-les-reseaux-sociaux-la-force-barkhane-est-visee-par-une-campagne-de-fausses-informations/.

Rumours about so-called organized fanatics serving undercover in the Armed Forces serve to spread suspicion within the units. Although some former members of the French armed forces have in fact joined the Islamic State to conduct holy war (jihad),[11] most Muslim soldiers are loyal to the French state. Indeed, a famous fake piece of news, which has been shared for years on several websites, deals with a so-called mutiny onboard the aircraft carrier *Foch* in 1999. According to this rumour, Muslim sailors, fed up with the bombing campaign against Kosovo (a now Muslim country) they were participating in, attempted to revolt. However, this never actually occurred.[12]

For all that, some potential Islamic terrorists and violent radicalized individuals have certainly been detected for years in the French armed forces and police. We must admit the enemy is competent in using new media tools and establishing communication strategies, capable of expressing himself ever more undisguised in the most efficient ways possible on the Web. Indeed, the design and production of some propaganda films and magazines do conform to Western standards.[13] Webzines like *Dabiq*, *Rumiyah*, *Inspire*, and *Dar al-Islam* were issued irregularly in 2014–2016 in several languages, including French. They provided starter packets to potential terrorists who could obtain technical and ideological material just by reading them. The defeat of the Islamic state as a territorial entity has not put an end to their sharing information or propaganda on the Web or the relevant digital support media.

A Deadly Threat to French Security Forces

The terrorist threat to the homeland has made military men anonymous in their own country. Nowadays, wearing the uniform has been banned outside the service. Names are erased

[11] The Centre d'Analyse du Terrorisme has identified approximately thirty former French military who have either joined the theater of operations on the side of terrorist organizations, primarily in the Iraqi-Syrian zone, or have participated in terrorist operations in France. See Manon Chemel, "Les militaires français et le djihad," Centre d'Analyse du Terrorisme, December 2019, http://cat-int.org/wp-content/uploads/2019/12/CAT-Militaires-Djihad.pdf.

[12] Guillaume Daudin, "De fausses preuves d'une infiltration islamiste de la Marine nationale," *AFP Factuel*, October 18, 2019, https://factuel.afp.com/de-fausses-preuves-dune-infiltration-islamiste-de-la-marine-nationale.

[13] Alexis Marant, *Studio de la terreur*, Canal+, 2016.

and faces are blurred to prevent identification during media coverage. As a result, soldiers have vanished from everyday life and from peoples' mind. With the exception of the seven to ten thousand soldiers of operation Sentinelle who patrol the streets to ensure the security of sensitive areas—mostly religious sites—French people can no longer see soldiers dressed in battledress or uniform in a bakery or shopping in a supermarket. Some retired military officials and anonymous senior officers do denounce what they consider a retreat in front of the enemy. Such an argument is not without merit. However, we must admit that over the past decade, members of the armed forces and other security services have suffered heavily from terrorism. Let us just remind three famous cases in France illustrating how service men have been targeted in today's war against terrorism on home soil. In all three cases, cyber security played a key role.

The Merah Case, 2012

Mohammed Merah was a chronic offender well-known to the French homeland security services. A radicalized Muslim, he had traveled several times to Pakistan and Afghanistan to pass through traineeships in terrorist boot camps. Although he pretended—and was eventually believed—to be traveling to the region as a tourist, some homeland security analysts continued to monitor his activities. On March 11, 2012, he set out finally to criminally act out in pursuit of jihad, targeting servicemen. He was able to identify his first victim easily: the latter had posted an advertisement with a far too explicit description on a widely known e-commerce site. The serviceman, an airborne NCO named Imad Ibn Ziaten, wanted to sell his motorbike; in the ad, he explained that he had no choice but to get rid of it as he was frequently away from home. In conclusion, he wrote, "I am a serviceman." Merah feigned interest in the bike and arranged an appointment with Ibn Ziaten; upon meeting him, he denounced Ibn Ziaten as a traitor to Islam and killed him. Three days later, he attacked a group of servicemen who were passing by in a street at the gates of their military compound in Montauban. Two soldiers were killed and

another one was seriously injured. On March 19, 2012, he finally attacked a Jewish school, killing one adult and three children.

Identifying the perpetrator thanks to the Internet Protocol (IP) address he had used while connecting to the e-commerce site, the police launched a vast manhunt. Merah, who had dug himself in at home and resisted a thirty-two-hour siege, was finally killed in an assault. Five members of an elite police force were injured during the action. Afterward, several jihadist armed groups claimed responsibility for Merah's attacks. Even murkier, the unclear nature of the relationship between Merah and the intelligence services has generated controversies about so-called security gaps and unproven theories of collaboration.

The Slaughter of Magnanville

The second case happened on June 13, 2016, when a twenty-five-year-old terrorist named Larossi Abballa slaughtered a police officer couple in their home in Magnanville. The couple's three-year-old son was spared thanks to the intervention of another radical Muslim, with whom Abballa was chatting on Facebook live. As he was filming the killings to claim his membership in the Islamic State, Aballa questioned himself about what to do with the kid. The terrorist, who had been convicted three years earlier of assisting a terrorist plot, was shot a few hours after the murders by an elite police squad.[14] The reason why he decided to kill those two persons remains unknown. However, it seems he did not choose the couple randomly. Analysis of his cell phone revealed he had surveilled the area several times. Moreover, in October 2017, while searching the home of a woman suspected of complicity in a terrorism case, the police seized a USB pen on which they found the names of 2,626 police officers. Also included was a list of the names, identification numbers, and units of all the senior members of a police union (dated to 2008). All these police officers served in the homeland security services. As to how this information

[14] "Ce que l'on sait de Larossi Abballa, le meurtrier d'un couple de policiers dans les Yvelines," *France Info*, June 14, 2016, https://www.francetvinfo.fr/faits-divers/terrorisme/ce-que-l-on-sait-de-larossi-abballa-le-meurtrier-d-un-couple-de-policiers-a-magnanville_1499095.html.

had leaked—the sensitive data had been shared with all the agents mentioned in the list and with the union itself, making the breach of information all the easier.[15] Indeed, the suspect had been housed by a close friend's mother who was an NCO police officer and union representative who had converted to Islam. The police interrogated her regarding the Magnanville slaughter, as she did know people about to participate in jihad.[16] However, due to a lack of evidence, no charge could be laid against her.

Harpon Case, 2019

On October 3, 2019, Mickaël Harpon, a civil servant working at the Intelligence Bureau of the Paris Prefecture, assassinated three policemen and an administrative agent in the courtyard of this institution, whose purpose includes preventing terrorism. There was no doubt in classifying the killing as a terrorist attack, since its perpetrator's aim was to "« kill unbelievers."[17] For the very first time, France faced a "blue on blue" terrorist attack, a friendly fire attack carried out on purpose by a member of the force.[18]

In the Harpon case, the most serious thing is that he had access to classified data, as he was a technician responsible for the maintenance of computers. In spite of his evident radicalization, the terrorist could consult lots of personal data concerning Prefecture employees. Confidential data as well as jihadist propaganda were found on his USB pen. While subsequent investigations could not confirm there were leaks of confidential data, this was due only to an

[15] "EXCLUSIF. L'identité de 2 626 policiers de la DCRI aux mains d'une radicalisée," *Le Point*, April 10, 2018, https://lepoint.fr/societe/exclusif-les-noms-de-2-626-agents-du-renseignement-aux-mains-d-une-radicalisee-10-04-2018-2018-2209549_23.php.

[16] "Une clé USB avec les noms de plus de 2000 fonctionnaires de police retrouvée chez une jeune femme radicalisée," *France Info*, April 4, 2018, https://www.francetvinfo.fr/faits-divers/terrorisme/policiers-tues-a-magnanville/une-cle-usb-avec-les-noms-de-plus-de-2000-fonctionnaires-de-police-retrouvee-chez-une-jeune-femme-radicalisee_2699414.html.

[17] Simon Piel, "Attaque à la Préfecture de police: Une recherche Internet faite par Mickaël Harpon accrédite l'hypothèse terroriste," *Le Monde*, February 26, 2020, https://www.lemonde.fr/societe/article/2020/02/26/attaque-a-la-prefecture-de-police-une-recherche-internet-faite-par-mickael-harpon-accredite-l-hypothese-terroriste_6030930_3224.html.

[18] In 2012, the French army experienced a "green on blue" attack caused by an allied Afghan soldier, who killed unarmed soldiers practicing sport at Guan FOB, Afghanistan.

absence of direct evidence.[19] In the aftermath of the killings, intelligence experts have publicly expressed concerns about how a well-known radical Muslim, who attended extremist mosques, could had been granted such a level of security clearance.[20] A special commission of inquiry has proposed thirty-five measures to prevent such a risk in the future.[21]

Conclusion

A misunderstanding of the cyber threat causes the human failures at the root of most security breaches in the armed forces and other security services (injury of reputation, compromising, attacks on members' lives). The recent cases underscore that one need not be a senior hacker or employ high-tech to cause losses. Increasing controls may produce no results if no one observes the procedures. However, a powerful and long-term awareness raising campaign aimed at informing servicemen on the cyber threat is starting to yield encouraging results, as a change in mentality can be observed. Indeed, cyber security has become quite inevitable in the everyday life of servicemen.

To face these new threats, France has taken various measures. First, its intelligence services have had to adapt to the e-revolution. Within the intel world, new departments and cells dedicated to very specific know-how have been set up. Along with the external intelligence service (DGSE) and the Military Intelligence Service (DRM), the Department for Intelligence and Defense Security (DRSD) seeks specifically to protect all MoD servicemen and cells. Dedicated to counterintelligence, its aim is to identify opponents' intentions and to neutralize any internal and external threats which may lead to hostile acts from organizations, groups, or individuals. DRSD agents investigate and protect. They identify weaknesses and contribute to

[19] "Attaque à la préfecture de police: Pas de trace de fuite de données, la clé USB toujours analysée," *Europe 1*, October 9, 2019, https://www.europe1.fr/societe/attaque-a-la-prefecture-de-police-pas-de-fuites-de-donnees-la-cle-usb-toujours-analysee-3924453.

[20] Jean Chichizola, "Affaire Harpon: La commission dénonce 'une faille majeure,'" *Le Figaro*, May 3, 2020, https://www.lefigaro.fr/actualite-france/affaire-harpon-la-commission-denonce-une-faille-majeure-20200305.

[21] "Attaque de la PP: La commission d'enquête fait 35 propositions pour répondre aux 'failles,'" *L'Express*, October 6, 2020, https://www.lexpress.fr/actualite/societe/attaque-de-la-pp-la-commission-d-enquete-fait-35-propositions-pour-repondre-aux-failles_2127862.html.

bolstering security. Among others, one of the key missions of the DRSD is to mentor troops on counterintelligence (securing data, preserving secrecy, avoiding reputational damage) prior to any tour of duty overseas. Every year, several servicemen are punished by the military high command, and sometimes by the courts, for judicial misconduct because of offenses that intel services managed to identify or prevent.

Nowadays, most electronic communications are encrypted. The armed forces use dedicated email and computer networks that are supposed to remain unbroken and hermetic to hackers' assaults. Today, any platoon leader frequently uses encrypted software to communicate within his own unit. Moreover, the MoD has been hiring hundreds of computer science specialists, software designers, data analysts, hackers, and other kinds of "geeks" to join ancient and brand-new units such as the 44th and the 54th Signal battalions, the 805th Signal company (created in 2016), which stands alongside the 785th electronic warfare company in Brittany, as spearheads for cyber security and counterintelligence. Even if much still must be done to compete with superpowers on the virtual battlefield, France has remained credible in how it understands the strategic issues. Hopefully, considering its indigenous know-hows and the renowned multinational defence groups (Dassault System, Sagem, Safran, Thalès, etc.) based in France, the issue is rather more "we will do it" than "we can do it."