Chapter

Cyberspace and Artificial Intelligence: The New Face of Cyber-Enhanced Hybrid Threats

Carlos Pedro Gonçalves

Abstract

While, until recently, cyber operations have constituted a specific subset of defense and security concerns, the synergization of cyberspace and artificial intelligence (AI), which are driving the Fourth Industrial Revolution, has raised the threat level of cyber operations, making them a centerpiece of what are called hybrid threats. The concept of hybrid threat is presently a key concern for the defense and security community; cyber-enabled and cyber-enhanced hybrid operations have been amplified in scope, frequency, speed, and threat level due to the synergies that come from the use of cyberspace and machine learning (ML)-based solutions. In the present work, we address the relevance of cyberspace-based operations and artificial intelligence for the implementation of hybrid operations and reflect on what this cyber dimension of hybrid operations implies for the concept of what constitutes a cyberweapon, the concept of hybrid human intelligence (hybrid HUMINT) and possible responses to the hybrid threat patterns.

Keywords: hybrid threats, cyber psychological operations, hybrid HUMINT, artificial intelligence, strategic studies, intelligence studies, data science

1. Introduction

The concepts of *hybrid threat* and *hybrid warfare* are, presently, key concepts within strategic studies[1] and intelligence studies[2], with a core relevance in the new defense and security context that was enabled by the twenty-first century's Fourth Industrial Revolution, driven by the synergization of *cyberspace* and *artificial intelligence* (AI), fueled by the accelerated and disruptive exponential expansion of machine learning (ML) [1–3]. Cyber operations, presently, constitute a key determinant component of *hybrid strategies* and *tactics* that configure the profile of *hybrid threats* and *hybrid warfare* [1]. *Hybrid strategies*, in the twenty-first century, involve the use of *Information and Communication Technology* (ICT) and AI tools to

[1] Strategic studies involve the study of strategy, crossing different disciplines, including military science, decision science, political science, and even systems science, and cognitive sciences.

[2] By *intelligence* we mean all the activities involved in the production of knowledge necessary to strategic and/or tactical decision. Intelligence studies are, then, the area of research that addresses all activities involved in such production of knowledge, including but not restricted to spying. The current chapter crosses, in permanent dialog, cyberspace studies, strategic studies, and intelligence studies.

combine conventional and unconventional operations, amplifying the impact of these operations [1–3].

In the current context of hybrid operations, there are, presently, three major dimensions of *hybrid strategic power*, understood as the ability to achieve one's strategic goals through *hybrid operations*, and these are:

- Network power
- AI power
- Cooperation power

The first type of power is enabled by social networks and the ability to use cyberspace for propaganda, disinformation, and viral campaigns in what constitutes a form of information-based warfare as well as for implementing cyberattacks that can disrupt different sectors as well as stealing (and possibly leaking) of critical data.

The second type of power involves the use of AI, in particular ML tools, as support tools for different cyber operations that may, in turn, support hybrid strategies. The range of AI applications can go from operations that take advantage of network power to cyber disruption of key infrastructures.

The third type of power is specific of today's defense and security environment, involving the cooperation of different state and non-state entities, the latter which include, for instance, organized criminal groups and terrorist groups that can cooperate with each other, supporting and enhancing each other's operations.

In the present work, we address the relevance of cyberspace-based operations and AI for the implementation of hybrid strategies and reflect on what this cyber dimension of hybrid operations implies for the concept of what constitutes a cyberweapon, as well as strategies that take advantage of the weaponization of cyberspace. We also address the concept of human intelligence (HUMINT) operations and their role in hybrid operations, in particular, how HUMINT was used in the past to support hybrid operations and can play a key role in the present; this leads us to the conceptualization of *hybrid HUMINT*.

In Section 2, we review main concepts linked to hybrid operations and address the strategic profile of hybrid operations in its different dimensions.

In Section 3, we focus on *cyber psychological operations (cyops)* as a major part of *hybrid strategies* and address how the use of AI and ML in *cyops* can be employed for the operationalization of hybrid strategies, targeted at weaponizing social networks, showing that AI constitutes a central driver of the future of these operations and allowing us to produce an assessment of the near future of hybrid threats, including a new face of *cyber terrorism*.

In Section 4, we address another dimension of hybrid operations and hybrid threats which is the role of HUMINT and the concept of *hybrid agent*, reviewing how HUMINT was used in the past for the implementation of hybrid operations and how it can be used in the present as a nexus for the successful implementation of these operations. In Section 5, we conclude with a final reflection on the role of cyberspace and the need for an extended concept of *hybrid resilience* as a way to face hybrid threats.

2. Cyberspace and the strategic profile of hybrid operations

Hybrid operations can be defined as the use of military and nonmilitary means to achieve one's strategic goals [1–3]. This means that rather than open battle,

one may use intelligence activities, subterfuge, and subversion in order to gain an advantage over the adversary.

Hybrid operations find a deep tradition in strategic thinking that can be traced back to the classics of strategic studies, in particular, to two of the main military classics of Ancient China [1, 4]: *Sun Tzu's Art of War* and *T'ai Kung's Six Secret Teachings*. These two works also inspired Japanese classical thinking about unconventional warfare and espionage and the use of specialized operatives that also implemented what can be considered today as hybrid operations. Operations with strategic and tactical dimensions were recorded during the transition from the Warring States period to the Edo period in different works. Of these different works, the *Sandai Hidensho* stands out, which consists of the scrolls that include the *Bansenshukai* [5], the *Shoninki* [6] and the *Shinobi Hiden* [7], these are three classical works on spying and on how to conduct subversive, covert, and unorthodox warfare, which also recognize the influence of *Sun Tzu's Art of War* and *T'ai Kung's Six Secret Teachings* [5–7].

While there is a deep tradition for hybrid operations in both Chinese and Japanese classics on warfare and spying, it is also important to stress that a thinking that is convergent with the Asian classics is also found in European Philosophical thinking about strategy and war, in particular in Machiavelli's *The Art of War* [8], which also addresses what are considered today as operations that fall within the scope of hybrid operations in books six and seven of this work.

In *T'ai Kung's Six Secret Teachings*, hybrid operations included corrupting key officials, using diplomacy as a weapon, compromising a kingdom's economy, alienating the ruler from the people, spreading rumors, and using propaganda and what is known today as psychological warfare [4]; similar operations are also described in the main Japanese classic on the art of spying, the *Bansenshukai* [5].

In what regards hybrid operations, the strategic action is not, thus, restricted to the battlefield but rather includes acting on the economic, financial, social, and political levels as a way to avoid open warfare or to weaken the adversary so that if open warfare does take place, one can easily win over that adversary [4, 5].

Specifically military hybrid operations are covered in the *T'ai Kung's Six Secret Teachings*, particularly in the *Dragon Secret Teaching*, in the section corresponding to the *unorthodox army*, and in the section addressing the *civil offensive*, in the *Martial Secret Teaching* [4], which is convergent with both the Japanese classics [5–7] and the European thinking [8].

One lesson that comes out of these classics of strategic studies and intelligence studies is the need for good governance and public policies as a way to guard against hybrid operations [4, 5], a point to which we will return in the last section of the present chapter. Disrupting governance goes to the key role of hybrid operations in classical strategy and intelligence thinking to undermine a country's governance and to make the people turn against the policymakers.

This is a point that is recovered in today's defense and security environment, present in different countries' military thinking. On the Russian side, as stressed by Chekinov and Bogdanov [9], two Russian Defense specialists, information technologies make the new face of warfare to be dominated by information and psychological warfare.

The central driving forces behind the twenty-first century's hybrid operations are *cyber psychological operations* (*cyops*), where *information superiority* plays a key role [1, 3, 9]. As stressed in [9], the new face of conflict is such that nonmilitary actions and measures are employed with ICTs used in order to target *all public institutions in a target country*. While this illustrates the Russian perspective on the twenty-first century conflict [1], we get a similar standpoint from Treverton [3], who is a former Chairman of the US National Intelligence Council. Treverton

identified, in the pattern of hybrid operations, typical information *cyop*-based warfare tactics, using propaganda, fake news, strategic leaks, funding of organizations and supporting political parties, organizing protest movements (taking advantage of social networks), using cyber tools for espionage, attack and manipulation, economic leverage, use of proxies and unacknowledged war and supporting paramilitary organizations.

While deeply rooted in the past thinking of strategic studies and in past military practice, the above references [1–3, 9] show that the renewal of the concept of hybrid operations and the relevance of this concept in the twenty-first century strategic thinking and doctrine come from the fact that these operations now have an effectiveness amplified by the use of cyberspace, which is a determinant factor in the change of the profile of the defense and security threats coming from hybrid operations; more properly, as it is addressed in [1], the twenty-first century hybrid operations can be implemented by both state and non-state agents, and this implies a major shift in strategic power, where individuals and groups, which may not be state-sponsored, can use cyberspace and even AI-based systems to implement hybrid operations that can have significant impact on a given country's governance [1, 2].

This adds a new dimension to hybrid threats, making the profile more complex from a defense and security standpoint, in the sense that we can have three types of hybrid operations' profiles:

- **Type 1:** state-sponsored operations implemented by a specific country or countries: these are implemented by countries and involve the human and technical resources of that country's Armed Forces.

- **Type 2:** non-state-sponsored operations: these are implemented by non-state agents and groups, not supported financially, politically, and logistically by any state.

- **Type 3:** state-sponsored operations implemented by non-state agents: the use of hackers and techno-mercenarism, the political, financial, and logistic support to non-state agents and groups opens up the way for the implementation of joint operations that involve non-state agents and different countries (with an added level of plausible deniability for countries).

These three types of operations are key for the characterization of hybrid operations. The *type 1 operation profile* has always been an integral part of strategic thinking and doctrine regarding unorthodox strategies and tactics and the way in which one may win one's goals without using conventional military forces, an approach that is considered in high regard within the context of the Chinese classics [4] and that is recovered also in the Japanese context of the employment of specialized operatives called *shinobi no mono* that were used as spies and specialists in covert operations, subversion, information warfare, and what are considered in the *T'ai Kung's Six Secret Teachings* as unorthodox ways [5–7]. Currently, however, cyberspace has amplified the effectiveness potential of these unorthodox ways, making hybrid operations a core dimension of military doctrine and the twenty-first century conflict, a point argued extensively in [1–3, 9].

However, the state-sponsored hybrid operations, implemented by a country's armed forces, intelligence agencies, or even specific *cyber warfare units* and, possibly, *hybrid warfare units*, are just part of the three types of hybrid operation profiles.

The *type 2 operation profile* is characteristic of a change in the strategic power dynamics due to cyberspace and availability of AI systems and is specific of the new defense and security framework of hybrid threats, namely, small groups, or even

a sufficiently knowledgeable individual, with sufficiently sophisticated hacking skills, can perform hybrid operations, taking advantage of cyberattacks and AI tools and target a country's governance, significantly disrupting that country with the same effectiveness as any state-sponsored attack. The threat ecosystem is, thus, no longer just one of the countries fighting each other but also of countries' governments and infrastructures being threatened by non-state agents that can implement hybrid operations as disruptive as any *type 1 operation*.

The key to the issue is the fact that cyber tools and even AI systems are freely available and the exponential trend linked to AI and ML and the increased usage of connected devices and smart government solutions open up the way for an exponential increase in the ability and opportunities to attack a country's governance with a low budget, this increases the disruptive potential of *type 2 operation profile*, which can be evaluated in terms of the increasingly low cost availability of means (including freely available bots and open-source malicious code dispersal), the increased dispersal of targets (due to the exponential trend associated with the Internet of Things (IoT)), and the ability to use cyberspace, including the dark web, to connect with like-minded individuals that are willing to support viral campaigns against specific targets.

Given the Fourth Industrial Revolution's foreseeable trend, the *type 2 operation profile* is typically a profile that involves most operations in cyberspace, given the high impact and low cost of these operations. The ability of sufficiently motivated individuals and groups, sometimes involved with criminal organizations, to successfully implement a hybrid operation with the same level of impact as a state-sponsored campaign is a point that only recently has been addressed in the literature on hybrid threats [1, 3, 10, 11], a point raised in [10]. This is a gap in that literature since there may be an underestimation of rapidly emergent threats. The main problem lies in the fact that hybrid operations can be implemented with significantly less investment, especially if their main component is cyberspace-based, and this can be considered as low-cost warfare or, as stated in [11], *war on the cheap*.

The Fourth Industrial Revolution has opened up the ability for weaker opponents, both state and non-state, to effectively engage opponents with stronger military forces, decreasing the comparative advantage of these stronger opponents. The network power and AI power allow for a non-state agents to launch a hybrid campaign on a targeted country from anywhere in the world, such that one may have difficulty in ascribing a given physical/national territory to the attacker and single out that attacker's country for a targeted conventional military response. A sufficiently sophisticated group can remain anonymous and even be transnational in the composition of its members, transitioning the defense problem from the traditional military dimension to a more complex response nexus of defense, intelligence, and law enforcement.

While *type 2 operation profile* is now being recognized as an increasing threat [1, 10, 11], with the tendency to increase in disruptive ability in the years to come, the *type 3 operation profile* has the potential for the most damage in that it involves the joint cooperation between state and non-state agents. This last operations' profile takes advantage of the cooperation power; cooperation in hybrid operations can take the form of cooperation between different non-state agents, including terrorist groups and different criminal organizations; between different countries; and between state and non-state agents.

The cooperation between state and non-state agents may become a main source of state-sponsored hybrid threats [10, 11]; rather than engaging in large-scale state-on-state conflict, different states can support non-state agents or act in a timing that is confluent with the actions of non-state agents, enhancing the ability of non-state agents to produce a large disruption on a targeted country's governance.

We are reaching a strategic context where both state and non-state agents can engage any given country by means of cyber operations, sabotage, espionage, and subversion [11], a point that also circles back to *Sun Tzu's Art of War* [4]. Hybrid operations, whatever their profile, allow an opponent or opponents to produce an imbalance of power, acting on the target's weaknesses, without engaging in conventional direct conflict and, possibly, even hiding their identities in the process.

The imbalance of power is linked, in Sun Tzu's thinking, to the concept of power as the ability to exercise one's authority and deliberative autonomy toward effective action; in this case, hybrid operations directly target a state's power by undermining its governance.

These operations can, in particular, take advantage of:

- Internal challenges to a state's governance by certain groups that wish to undermine a state's authority
- Failure of a state in adapting to society's concerns and its people's problems, being unable to respond to disruptions to the state's finances, economic problems, environmental problems, and social and political problems
- A view in a country's society that a regime has lost its legitimacy to rule

The above three targeted state-level weaknesses match what Margolis in [11] identified, respectively, as sources of three types of crises:

- ***Crises of authority*** that result from a state's inability to enforce its rule, not being able to control all of its territory, or becoming unable to enforce all its laws
- ***Crises of resilience*** that result from a state's inability to adapt to different disruptions
- ***Crises of legitimacy*** that result from society's view that *a regime has lost its right to rule because it is wrong or unjust*

These three types of crises can occur in a given country and be triggered by hybrid operations or amplified by well-timed hybrid operations, in particular, those that use information and cyberspace as a weapon.

Connecting the three profiles and crises, in **Figure 1**, we synthesize, in scheme, the links between the profiles of hybrid operations and the three types of crises identified by Margolis [11].

The *type 1* and *type 2 operations* are confluent with each other in the cooperation involved in *type 3 operations*. It is important to notice that, in some cases, a *type 1* or a *type 2 operation* can lead to a *type 3 operation*, and that the timing of a *type 1* with a *type 2 operation* can lead to a *type 3 operation* due to synchronized hybrid tactical actions. The three types of operations can all target the three weaknesses, authority, resilience, and legitimacy, amplifying state instability and leading a country into a crisis situation that may, in the limit, produce the fall of a government.

Now, regarding the means and vulnerabilities, it is important to stress that the Fourth Industrial Revolution also opens up the way for cyber-physical attacks, including attacks using drones and drone swarms, as well as cyberattacks on automated systems and cyber-physical systems; all these are dimensions of the wider cyber-enhanced synergy of conventional and unconventional operations that constitute the strategic and tactical ground for hybrid operations and that may predictably characterize the new level of hybrid operations in years to come.

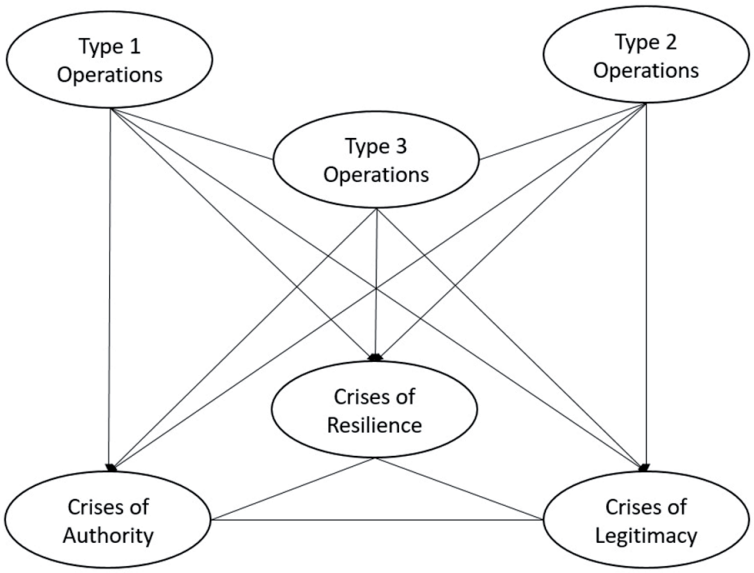

Figure 1.
Hybrid operations profiles and crisis profiles.

The other side, which we are already seeing today, is situated in the virtual space but still able to severely affect countries' governance; as stated above, this is the weaponization of cyberspace, using social networks and AI for hybrid operations. In this case, the actions are situated only in the virtual space, but they can have severe social, (geo) political, and economic consequences.

Platforms, in particular social networks, the manipulation of contents, and the use of AI, ML, and data science to manipulate people's behavior, online and offline, are a major component in these operations, and it is the subject of the next section.

3. Cyber psychological operations and hybrid threats

The strategic level of hybrid operations involves the definition of the main objectives for hybrid operations, the targets, and possible collaboration networks. The choice of resources and ways to combine them to operationalize the hybrid strategy depends upon the strategic deliberation. On the other hand, the means also condition the set of available tactics that may allow one to operationalize a given strategy.

The strategic power of hybrid operations in allowing for a state or non-state agents to achieve their strategic objectives has increased due to the resources available that allow for high yield with low investment; these resources are linked to the network power and AI power, defined at the beginning of the present chapter.

In what regards hybrid operations, the network power and AI power cannot presently be considered separately, since it is precisely the synergy of cyberspace and AI, in particular through ML, that determine the present strategic and tactical momentum of hybrid operations and that allow one to anticipate the future of hybrid threats. We now address one of the major components of hybrid operations, namely, information warfare and psychological operations using cyberspace.

Psychological operations (*psyops*) involve the use of different means and tactics in order to influence the behavior of target audiences. While, traditionally, *psyops* were employed by countries and constitute an integrating part of military doctrine, the expansion of cyberspace has led to the possibility of groups that are not part of

any country's official military branch to implement these operations. An example of this is ISIS' online propaganda as well as hacktivist groups such as anonymous online activities.

The use of cyberspace and hacking, including the defacement of a country's websites, the online dispersal of sensitive and/or compromising data through social media platforms, the possibility of using the *dark web* for the disclosure of sensitive data that can then be made public in the *surface web*, and the use of social media for propaganda and recruitment, for the denouncement of different causes, and for the manipulation of citizen journalism as a way to publish both true and fake news as well as to disperse other fake contents (including images, audio, and videos), all these are examples of ways in which *psyops* can be implemented using cyberspace, so, at present, *psychological operations* are an integral component of hybrid warfare in what constitute *cyber psychological operations* or *cyops* for short.

As stated previously, in the present chapter, *cyops* are a major part of hybrid operations, and *cyber psychological tactics* involved in *cyops* typically include [3]:

- *Propaganda* (in particular, dispersed online through social media)
- *Fake contents* (in particular, *fake news*)
- *Online dispersal of sensitive data* (*leaks*)

Each of these tactics takes advantage of network power, AI power, and cooperation power. There are three drivers that have amplified the effectiveness of the above tactics:

- The increased dispersal of connected devices, including *smartphones* and *tablets* that allow an easy and frequent access to the Internet
- Search engines and online services that adapt to each user's interaction pattern
- The growing use of social media over traditional media

Added to this infrastructural accessibility to these devices is the high frequency use of these devices and sometimes addictive component associated with this use, an addictive component usually linked to social networks.

A specific pattern of usage favors the dispersal of sensitive data, news, and general contents in social media: the fact that the online reading of social media contents usually does not involve a high level of reflection but rather engages the users in a way that is meant to be appealing and to be shared quickly with as most people as possible, users seldom read or reflect deeply on the contents that they are sharing, usually skimming through them and sharing the most appealing ones.

This is a pattern that is particularly useful for dispersal of contents that are presented in the form of scandals, sensitive information that was not known, conspiracies' denouncements, and so on. This point leaves a marker in data on fake content dispersal as shown in a study on the differential diffusion of verified (true) and false rumors on Twitter from 2006 to 2017, published in [12]. In the study, *politics* and *urban legends* stand out as the two categories with the highest frequency in rumor cascades.

The study concluded that rumors about politics, urban legends, and science spread to the most people, while politics and urban legends exhibited more intense viral patterns [12].

The study found a significant difference in the spread of fake contents vis-à-vis true contents, namely, true contents are *rarely diffused to more than 1000 people,* while

the top 1% of fake rumor cascades are *routinely diffused between 1000 and 100,000 people* [12]. The authors' results showed that fake contents reached more people at every depth of a cascade, which the authors defined as *instances of a rumor spreading pattern that exhibit an unbroken retweet chain with a common, singular origin*.

The result that fake contents *reached more people at every depth of a cascade* means that more people retweeted fake contents than true ones, a spread that was amplified by a viral dynamics. The authors found that fake contents did not just spread through broadcast dynamics but, instead, through peer-to-peer diffusion with viral branching.

Another relevant point, for hybrid operations, was that fake political contents traveled deeper and are more broadly reaching more people and exhibiting a stronger viral pattern than any other categories and diffusing deeper more quickly. This dynamics is not however due to users who spread fake contents having a greater number of followers; the study found exactly the opposite with a high statistical significance. In inferential terms, users who spread fake contents tend to have fewer followers, to follow fewer people, to be less active on Twitter, are verified less often, and have been on Twitter for less time. However, fake contents were 70% more likely to be retweeted than true contents with a *p-value* of 0.0 in Wald chi-square test.

The fact that user connectedness and network structure did not seem to play a relevant role in *fake content* dispersal made the authors seek other explanations for the differences in *fake content* versus *true content* dispersal. The authors reported that fake contents usually inspired greater number of replies exhibiting surprise and disgust. The authors' hypothesis is that novelty may be a key factor in *false rumor dispersal*.

However, there is a relevant point to take into account when looking at the study's results, which can be expressed by the following extreme example: an account with no followers and not following anyone can still get a high number of retweets and exposure on a content if it uses *hashtags* on hot topics and builds its tweet in a specific way that increases the probability of it being retweeted.

Moving beyond this specific study and considering social networks in general, working with the conceptual basis of strategic studies, we are led to introduce the concept of *tactical accounts*, defined as accounts that are created for tactical purposes in the support of a *cyop* strategy; these accounts can be managed by a single individual or staffs, and its operations can involve the use of *bots* that automatically generate contents with certain specifications, mostly aimed at making the contents viral in the spread.

The viral content design along with multiple accounts operated by *bots* are major tools for a *tactical account system manager*, that is, any operative can use multiple tactical accounts simultaneously to create a fake content dispersal so that it can gain momentum and become viral.

In general, fake contents can spread on hot topics by the use of *hashtags* or other means of dispersal, which diminishes the connectivity need for any single *tactical account*'s effective impact. Furthermore, from a *cyops'* standpoint, it is easier to *fly under the radar* by managing multiple newly created fake accounts that can even be managed by a single agent, who may then use these accounts to disperse fake contents incorporating *hashtags* on political issues and composing the messages so that they have an appealing emotive content, making it more likely for people to select them.

Returning to the study [12], the fact that the authors did not find strong evidence that algorithms were biased toward spreading of fake contents but rather that fake contents were being dispersed by people is favorable to the point of the way in which the message is built as the key factor in getting a fake content to gain traction. This point is echoed in [13] where it is argued that the belief in fake contents is driven by emotional responses amplified by macro social, political, and cultural trends.

Social media are particularly sensitive to the careful crafting of the message to fit viral conditions, in the sense that these media are managed by platform-based businesses, optimized for quick spread of information to reach target audiences and mass dispersal; in this sense, they are aimed by design at viral dynamics and addictive usage patterns that increase the interaction time with the platform and create value for these businesses.

The technology is thus an enabler of viral dynamics and, in that way, facilitates fake contents' dispersal by the way in which these contents are produced, in terms of the message that they contain, the emotional responses which they are aimed to evoke, and their timing and their management of conditions of dispersal (for instance, the use of *hashtags* on trending topics in Twitter); all this contributes to the increased likelihood that fake rather than true carefully crafted and reflection demanding content become viral.

Hybrid tactics can take advantage of multiple (*fake*) *tactical accounts* and use methods of automation of content generation, with possible applications of data science, in order to generate the content presentation that may be the most effective in getting people to adhere to and, thus, share. By working with data on viral tweets, ML algorithms may be trained in predicting the structure of a content that may make it more probable to become viral and use this to help a *cyops* operative design the message in order to make it more viral and then use *tactical accounts* to disperse it. Message contents, including *hashtags*, *emoticons*, and *gifs*, are useful tools in manipulating the message content to better fit a target audience [14].

Another way to manipulate viral content dispersal is cyberattacks aimed at compromising search engines and recommendation engines in order to disperse fake content that fits the goals of an intended *cyop*.

Search engine poisoning or even a more sophisticated *search engineering* has been applied in the past by *black hats* to spread malware and fake contents [15, 16].

There are various methods employed in this last context that can be highly effective for hybrid operations: the first is content injection in websites, online forums, and social media in the form of spam posts that can also point to specific websites used within a *cyop*; this is a task that can be automated.

A second level is the creation of networks of websites and social media accounts that spread alternate media messages and that reinforce *echo chambers* for specific content that can, thus, become viral, taking advantage of a concerted social media campaign that divulges these accounts.

The sharing of these accounts can, in turn, become viral and link to different alternate media websites that can be used for *cyops* and manipulate a user's web search and interaction with different content platforms. If, in the interaction, with any search engine and content platform, there is a powerful algorithmic adaptation to each user's pattern, then, any user, influenced by viral content, will have a tendency to be fed back the content that the *cyop* is aimed at. In this way, by strategically using viral dynamics, a *cyop* can manipulate a vast amount of users and engineer massive *echo chambers* where massive amounts of users get personalized content that fits the *cyop* in question.

In this case, the hacker or hackers do not need to compromise the AI systems that manage a social media platform; rather, they are *hacking people's behaviors* and are taking advantage of the effectiveness of the platform's own AI systems in adapting content to user interaction profile. Since the way a user interacts with a platform leads to a specific response on the part of the platform for automatic user personalization, each user gets his/her own experience; however, the commonality of usage patterns allows for collectives of users with common tastes to receive similar or confluent viral contents.

Creating and financing tactical networks of social media accounts amplify this *hybrid strategy*, as long as the platform adapts very quickly to a user's profile facilitating the *echo chamber engineering* needed for the *cyop* to be successful. Similar tactics can be employed on any type of social network. However, of the different online media platforms, Facebook seems to stand out in terms of effectiveness of fake news dispersal, with a higher frequency of cases of visits to fake news websites occurring near a Facebook visit, as reported in [17].

Besides content injection in *blogs*, *forums*, and *social media*, another way for search poisoning involves content injection in compromised websites, as well as search redirection. Search redirection attacks employ sites that have been compromised to be used in a search redirection operation and whose owners usually do not suspect that their website has been compromised [16]. These *source infections* in turn redirect to traffic brokers that redirect traffic to specific destinations that fit the hackers' main goal [16]. Currently, ML algorithms are being trained against redirection as a defense against it [18]; however, ML algorithms and data science can also be employed to manipulate content, including written text, pictures, and even videos. In the foreseeable future, a higher ability of *deep fake videos* to fool people may greatly enhance the impact of fake content dispersal.

While disinformation and propaganda, through online fake content and propaganda dispersal operations, have become highly impactful in terms of their strategic and tactical value [3, 17], there is another level of *cyops* that may be implemented by any state or non-state agent that can have a strong impact on society. This is exemplified by the *Blue Whale Challenge*, which is an example of the power of what can be considered a *gamification attack*.

Gamification attacks use the Internet to introduce a game which leads the players through a series of challenges down a path where those players are led to either self-harm or even murder. In the case of the *Blue Whale Challenge*, the players were led to self-harm. The game involved a series of life-threatening tasks given to players by a curator, and each player had to fulfill these tasks which ended with the suicide of the player [19]. In a certain sense, this constitutes a cyberspace-enabled form of murder, by leading a person to commit suicide. The *Blue Whale Challenge*'s curators can be treated as a new breed of serial killers that use the Internet for psychological and physical torture, eventually leading their victims to kill themselves as the endgame of the tasks that they give their victims.

If we replace the final task of *suicide* with a final task where the player has to *murder* someone else or even a number of people, perhaps even in exchange for the player's own life (an *either kill yourself or commit murder* option), then, the *Blue Whale Challenge* becomes the first example of designing a web game that can lead not only people to suicide but also to murder on a scale and intensity that can be comparable to those of standard terrorist networks.

One should stress that this is a form of *cyops* that can easily be engineered by someone not affiliated to any terrorist group. A single person can take advantage of the power of cyberspace and of social networks to create such *challenges*; furthermore, even if the individual is caught and arrested, the game can go on independently of the individual, where anyone can become a *curator*. The game itself becomes the terror referent and the platform for terror practices.

This breaks with any traditional approach to engaging and handling terrorist organizations, since a *terror game* can be played by anyone, without any political goal, without any political affiliation, and with no end other than the exercise of violence. These new serial killers that become curators of these games can be caught and imprisoned, but the game can go on with different iterations. There is a form of digital autonomy and continuation of a *terror* game as a collective dynamics that is sustained by its players, but that goes on despite the catching of particular curator players, as

long as it is available for playing; the game can even come back with new variations and remain, and even if it has no players, it can be played again at any time.

This is not a *terror network* that one can address with traditional tactics; it is a *terror game*, and the *Blue Whale Challenge* is just the first example of this. The game becomes the *referent* for any players, who may never have physically met. Systemically, the game becomes a *dispositional driver* for a typological order of cyber-enabled terrorist practices. Another point is that, potentially, such *terror games* can be sustained by non-humans, that is, by AI systems, and even if all human curators were caught and arrested, *bots* could take over and play the same role as a human curator (the player that abuses the other players). In this sense, a single individual, using AI systems, can create *terror games*, sustained by an "army" of *cyop bots* that will be difficult to stop. A new breed of the twenty-first-century serial killers can become a source of new cyber-enabled terrorism that uses *gamification* as a way to resiliently murder on a global scale, with an impact on par with that of major standard terrorist organizations.

The reason why *bots* can be used here as *cyber psychological weapons*, in such *games* as the *Blue Whale Challenge*, is linked to the algorithmic basis of these games' approach; in particular, the behavior of curators can be algorithmically replicated by *cyop bots*. Indeed, the process involves using social networks to search for young people who fit specific profiles, which can include being depressed or showing addictive behavior. The list of tasks includes dynamics that introduce sleep deprivation, listening to psychedelic music, watching videos with disturbing contents sent by the curator, and inflicting wounds on one's body, among other tasks [20]. The tasks follow a prescribed set of steps that lead the victim into a disturbed mental state and susceptible to the influence of the curator, the victim is a target of a form of *cyop* that falls within a pattern that can easily be turned into an algorithm.

The *gamification* of *cyops* in terror operations is in its infancy; however, the tools available to it are amplified by the IoT, mobile devices, and platform usage. In the *Blue Whale Challenge*, we see a new tactics based on platform weaponization, that is, the use of platform-based businesses to compromise its users and eventually lead to their deaths (in the case of the *Blue Whale Challenge*) or even to the killing of others (if instead of suicide the player is led to kill others).

Empowered by *cyop* bots, a small number of individuals, or even one individual, can create a game that may go on independently of them; the game can persist as a dynamics that continues to be played in the platform, which functions as a replicator for the deviant and predatory behavioral patterns needed for the *terror game to go on*. Having been played once, the dynamics that characterize the game can always come back; in this sense, the platform works as a way for the digital continuation of the terror game.

This is very different from the case of a terrorist network that has a hierarchical structure and that has cells and individuals that play different roles within an organization.

A *terror game* is just a set of behavioral patterns, with algorithmic components, that can be replicated like a form of social virus which goes on as long as there are players. There is no stable hierarchy and no cells and no individuals that can be targeted which may harm the game, because the game has a virtual fluid existence that can be perpetuated as a dynamics to be retrieved any time, any place.

The *terror game* is characteristic of a side of platforms, especially social networking platforms that make them highly weaponizable, namely, platforms are means for the exercise of biopower in the sense of Foucault [21], a point that is convergent with the issues addressed in [22].

Platforms can function as means for the exercise of control, reward, and punishment and of manipulation of its users' desires, fears, and sources of inclusion and exclusion, integration and segregation, connection and isolation, and friendship and bullying.

By increasingly sharing one's life in platforms and by using integrated systems, in particular IoT devices, the new stage of the Internet revolution is such that any heavy user of these systems can be *datafied*, profiled, and manipulated by hacked devices (including hacked AI systems) and manipulated by predators that use fake accounts and their victims' profiles to launch directed *cyops* that can, in the end, as was the case with the *Blue Whale Challenge*, lead to a person's death.

According to data, reported in [20], Instagram ranks higher in posts than the Russian VK social network (which was where the game spread initially) and Twitter. On Twitter, the large majority number of posts related to the *Blue Whale Challenge* was identified by the authors as coming from *smartphones* with the Android OS, which shows how mobile devices are useful in feeding *terror gamification* operations.

Another pattern revealed in these authors' research is a key common factor in online *cyop* campaigns. In particular, many accounts talking about the *Blue Whale Challenge* were new accounts with not many followers; this shows again the possible use of *tactical accounts*. This is a basic necessary tactical choice for predators operating online, who will want to hide their identity; furthermore, in order to gain online traction on a *cyop*, the use of multiple *tactical accounts* is a necessary step. Thus, just as in *state agents*, *non-state agents*, including *cyber-enabled serial killers*, may tend to use multiple *tactical accounts* in online platforms when addressing their targets.

The use of challenges like the *Blue Whale Challenge* and the *Momo Challenge* directly targets a large amount of victims and constitutes a security and law enforcement problem [23].

Returning to *cyops*, whatever their profile, these are currently about using cyberspace and ML for *hacking people*'s behaviors. In this sense, while a *cyop* against a given country may take advantage of resilience, authority, or legitimacy vulnerabilities, the increasing use of the platform-based technologies, managed by ML algorithms, where each user's data is exposed and available for exploitation, leads to another level of vulnerability which is the ability to use citizens' own data and behavioral patterns against them or to manipulate citizens into patterns of behavior that interest a given state or non-state agent.

The fact that *cyops* have certain components that are algorithmizable implies that one can program bots as *cyop* weapons that function as a form of new computer virus, a behaviorally conditioning content-based virus that is aimed at hacking people's behaviors, delivered through platforms for both mass exposure and personalization. The current trend of using algorithms for decision-making and in everyday life, integrated in platforms and that feed on each user's data and adapting the service and contents to each user's profile, makes AI weapons, employed in *cyops*, increasingly effective tools.

While the *cyops* that were discussed above include the creation and manipulation of contents to produce responses and manipulate people's behaviors, the impact of these contents can become even more amplified if the dispersal of these contents is timed with the leak of true contents. In this case, people tend to believe the fake content that is consistent with the true content. The leak of true content can initiate a fake content campaign, where the true content provides the context for the fake contents that will be used in the fake content campaign.

In this case, *leak platforms*, like *WikiLeaks*, can be used by hackers, whistleblowers, as well as other agents (state and non-state agents) to disperse true content and provide the timing for initiating fake content campaigns. However, besides *leak platforms*, there

is another level of hybrid operations which also increases the threat of these types of operations for any country; this is the new *hybrid human intelligence/counterintelligence (CI)* context, in which the concept of a new field agent is a key factor.

4. Hybrid HUMINT

The concept of human intelligence involves a twofold dimension: to gather information from human sources that are not HUMINT operatives and to gather information from HUMINT operatives. In terms of operations, HUMINT involves [24]:

- The clandestine acquisition of relevant data
- The overt collection of relevant information by people overseas
- The debriefing of foreign nationals and citizens who travel abroad
- Official contacts with foreign governments

While budget restrictions, the cyberspace expansion, and the development of data science have fueled the interest in signals intelligence (SIGINT) and open-source intelligence (OSINT) and led to some divestment in HUMINT, considered, for instance, more expensive in terms of time and resources involved than OSINT, an approach that considers an opposition of HUMINT *vs* OSINT and HUMINT *vs* SIGINT is the wrong way to look at things from an *intelligence/counterintelligence* effectiveness standpoint, within the new defense and security context, characterized by the critical threat of hybrid operations.

In fact, one can robustly argue, from a technical and technological standpoint, that HUMINT is a major centerpiece driver of hybrid operations, a nexus around which SIGINT and OSINT can be leveraged, with the new agents on the ground being able to both gather strategic and tactical information, implement (cyber) subversive maneuvers, steal data, and even compromise critical systems of any organization.

In the new context of hybrid operations, a new breed of HUMINT operative is not only a spy but also a hacker and a hybrid operations specialist that can infiltrate an organization and bring it down from the inside. We call this the *hybrid agent*.

From a *counterintelligence* standpoint, the new dimensions of the threat of covert human agents need to be critically addressed. The first thing to stress is that the threat level is very high for any state; on the other hand, the operational advantage of the new breed of HUMINT operative is also very high, so that, from an *intelligence/CI* standpoint, states need to invest in both these new *hybrid agents* and to find countermeasures for them.

To fully realize the implications and measures of the concept of a *hybrid agent*, which is the main point of this section, we need to first address some conceptual dimensions from intelligence studies and strategic studies, since while the tools of the *hybrid agent* have changed and the profile and impact is new, there was an old case of a form of *spy* that fit this profile of *hybrid agent* which was employed in Japan's Warring States period (*Sengoku Jidai*) and later in the Edo period. This old *hybrid agent* fits a similar profile and role that the new *hybrid agent* may come to fit in the years to come.

During the *Sengoku Jidai*, spies were mainly employed from the Samurai and Ashigaru classes, but progressively, especially in the Iga and Koka provinces, spying was systematized, developed, and integrated in a body of knowledge and skills that were taught to warriors, a body of knowledge that was built on top of the warrior normal training.

Different regions and Samurai clans also had their trained spies. It is important to stress at this point that there coexisted two types of spies in Japan: warriors who were employed as spies but that were not trained spies and warriors who, besides their normal martial training, were trained as spies. Another division that arose was between the trained spies that were a part of a Daimyo's army and thus served the Daimyo and the spies for hire, mercenary spies.

Due to their skills, Iga and Koka spies became mercenary spies, that is, spies for hire that also operated based on alliances of these regions with different groups. It is important to consider what constitutes the body of knowledge that the Japanese incorporated in what they considered to be the *art of spying*, called *shinobi no jutsu* or *ninjutsu*, erroneously addressed in popular culture as a martial art, as assassination, and/or as warriors that opposed the samurai, all incorrect misconceptions [25].

The fact that traditional scrolls on this body of knowledge are hard to track down, being, in many instances, in private collections, in some way contributed to the misconception to be perpetuated and has produced a gap in the literature on intelligence which usually cites *Sun Tzu's Art of War* but overlooks, in the study of the history of intelligence, the deep development of the theory, strategies, and tactics of intelligence that is present in the traditional texts on *shinobi no jutsu*, which, as a relevant point in dispelling the misconception, never cover any kind of hand-to-hand fighting techniques [5–7, 25, 26].

Recently, thanks to the efforts of the historian Antony Cummins and Yoshie Minami, the major texts are now translated into modern English, and Cummins has tracked down scrolls beyond the main known texts and translated them to English, making them available to the wider audience.

These texts allow people, researching in intelligence studies, to find new references that deepen *Sun Tzu's Art of War*'s last chapter. These works, in particular [5, 26], develop in great detail a full body of knowledge in what the Japanese considered the art of spying and operationalize *Sun Tzu's Art of War*'s last chapter into a detail that provides an insight into the history of intelligence.

The relevant point is that these works on *shinobi no jutsu* introduce a profile of an operative, the *shinobi no mono*, which is largely a *hybrid warfare specialist*, and also constitute some of the few examples of classical works that are only devoted to intelligence, that is, these are some of the few examples of *Classical Intelligence Manuals* that form a compendium of the main strategies and tactics of intelligence in Japan's Warring States and Edo periods, some of which hold, in terms of their main patterns and principles, for any period and place.

If one analyzes these different classical Japanese works on what are today called intelligence studies [5–7, 25], one finds that, in Japan, the *art of spying* (*shinobi no jutsu*) included, among other specialized knowledge, a core of areas of expertise that, under close scrutiny, are generalizable to other countries and historical periods [27], and these areas include:

- Military strategy and tactics
- Scouting
- Infiltration and tactical disruption
- Unconventional warfare, including deep knowledge of subversive maneuvers and psychological operations
- Deep knowledge of counterintelligence

Infiltration came in two ways [5]:

- *Yojutsu*: which involved infiltrating the enemy in plain sight, that is, using long-term undercover agents
- *In jutsu*: which involved stealing in, hiding from the enemy

In jutsu was largely employed during the *Sengoku Jidai* and already included the conventional and unconventional, where the trained agents infiltrated the enemy ranks, usually at night and used fire and unconventional tactics to disrupt the enemy in a way that allowed for a well-timed conventional open attack to ensue. These were the precursors of battlefield hybrid operations and are documented in detail in the *Bansenshukai* [5].

Yo jutsu usually needed someone with some level of scholarship, namely, from the Samurai class. This was the long-term undercover operative, which not only gathered information just like any HUMINT specialist but also employed subversive maneuvers, disinformation, counterintelligence, and political manipulation. One finds an example of this in the *Bansenshukai* [5], which reportedly is an Iga manual, but that may also contain a synthesis of Iga and Koka knowledge, where it is stated that an agent needed to obtain and keep copies of the marks and seals of the lords of various castles so that these could be used to forge letters in order to incriminate a target for conspiracy. Using agents to frame key people sow discord among the enemy's ranks and even for assassination (in particular, through poisoning).

Undercover operatives (using *yo jutsu*) were employed for disrupting the enemy's intelligence and decision-making process (disinformation), making false charges, spreading rumors (the dispersal of fake contents was already present in this period), and sowing domestic conflicts, discord, and doubts among the enemy's vassalage, as well as for setting fires or causing confusion among the enemy's castle in order for an open strike to occur. These are documented in the *Bansenshukai* [5] and are all parts of hybrid operations. Indeed, the play between the conventional and unconventional which is a key characteristic of *shinobi no jutsu* is strongly convergent with the two the major Chinese classics of strategy: *Sun Tzu's Art of War* and *T'ai Kung's Six Secret Teachings* [4], the latter which is considered in [5, 7] a Chinese reference on what the Japanese called *shinobi no jutsu*.

The Japanese knew of both works, and they are referenced in the different Japanese classical texts on *shinobi no jutsu* [5–7, 25, 26]. In particular, Sun Tzu's five types of agents were employed and elaborated upon in terms of intelligence strategies and tactics in the context of the Japanese classics, and these five types are [4]:

- Local spies (employing of locals to gather information)
- Internal spies (employing people who hold government positions)
- Double agents (employing the enemy's agents)
- Expendable spies (employed to spread disinformation outside the state; in the Japanese case, they used these in conjunction with the highly trained undercover operatives, which, due to their training, were not considered expendable but were, rather, high-valued assets that were used for what are today considered the core of hybrid warfare: disinformation, psyops, fake content and rumor spreading, sowing discord and unconventional strategies and tactics, besides spying per se)
- Living spies (who returned with their reports)

In [26] these five types of spies are explicitly addressed with an in-depth analysis on the strategies and tactics that are involved in their usage.

To these five types, one can add another type, which holds a key value for the new hybrid operations' context: the unwitting agent, who is supplying information for the enemy but is unaware of this fact. One can already find this type of agent in some passages of the *Bansenshukai* [5].

Now, taking into account this historical context, let us consider what we called the twenty-first century *hybrid agent*, which, in terms of operational profile, is used in the same manner as the *shinobi no mono*, namely, we have an expert in strategy and tactics that can be infiltrated in an organization (*yo jutsu*) and who will be used to both gather critical information (the standard classical HUMINT aspect) and find the main vulnerabilities of the target organization and, if given the activation order, is capable of disrupting the organization from the inside using cyberattacks, compromising key employees, releasing compromising data, and/or launching a fake content campaign against the organization.

Mirroring the setting of fire and the compromising of the intelligence cycle used in Medieval Japan, we now have the possibility of a long-term undercover operative to physically install malware and cyberweapons and hack critical systems to corrupt key data and disrupt the organization's normal functioning.

Business, banking, healthcare, and government are particularly vulnerable sectors that can be hacked in this way. The businesses' use of ML-supported OSINT can be compromised by malware aimed at attacking the ML infrastructure and thus corrupt strategic decisions, business secrets, and strategically sensitive data which can be stolen to undermine a target country's business (state-sponsored corporate espionage) either by using these data for gaining a negotiation leverage, an R&D and competitive advantage or, simply, to disclose it, bringing losses to these businesses.

Companies and banking that employ platforms, in the new 4.0 paradigm, can have their platforms compromised by a *hybrid agent*, undermining the stakeholder confidence.

If there are corruption practices or any key figures in key business, banking and/or political sectors fall prey to entrapment (even digital entrapment); then, this can be used to disrupt a country's business, banking, and even political sectors, even to turn the people against these sectors in well-orchestrated hybrid campaigns that use social networks to amplify the disruption effect. The principles behind this *economic and political warfare*, which is a key dimension of hybrid strategies, are expanded in detail in *T'ai Kung's Six Secret Teachings*.

Our main point is that the new *hybrid agent* is a key player in making this type of hybrid operations effective. The reason for this is that while remote hacking, SIGINT, OSINT, and even *cyber intelligence* (CYBERINT) can be effective, the *hybrid operative* is more disruptive and may greatly enhance SIGINT, OSINT, and CYBERINT; there are a few reasons for this.

Hacking an organization becomes exponentially more effective if it is done by someone who is undercover inside the organization, and this person can have direct access to an organization's critical systems and compromise them by physically installing malware. Social engineering also becomes easier and more effective if combined with direct personal interaction with human targets that can be hacked. Hacking colleagues' smartphones, for instance, and other IoT devices can lead to a new form of *unwitting agent*: the person who takes his/her devices everywhere, devices that can be accessed by the *hybrid operative* and used to record audio, video, geographical data, and other personal data. This means that conversations can be recorded, video can be recorded, and even personal data can be gathered and used to compromise a target individual.

With increasing sensorization of organizations, a successful *hybrid operative* can turn the organization's *sensorization* systems into his/her own listening devices. Furthermore, standard HUMINT can be combined with OSINT and SIGINT, where the *hybrid operative* can directly interact with a human target, hacking the target's devices, employing social engineering tactics, and then combining the cyber intrusion with fake social network accounts, managed by a remote team that may follow the target on such places as Facebook, Twitter, Instagram, and so on, further interacting with this human target, using the social media, private chat systems, and even video chat sessions with remote support team operatives, in order to manipulate the target and find the target's weaknesses, gaining the target's confidence and possibly compromising the target or using that target as an (unwitting) source of information.

The trained *hybrid operative* must then be:

- An expert in *cyops*
- An expert in *hybrid operations*
- A hacker with strong skills in social engineering

From a CI standpoint this is a major threat on two fronts:

- On the state-sponsored front: the *hybrid operative* is a key nexus for combining synergistically HUMINT, OSINT, SIGINT, Social Network Intelligence (SOCINT), CYBERINT, and *cyops*, taking all this to a new level which can seriously disrupt a country's key public and private organizations.
- On the non-state-sponsored front: a very skillful hacker team or even an individual hacker, with strong social engineering skills, who have physically infiltrated a target and are supported by *bots* that automate the fake content dispersal, can, with very low cost, produce the same effect as a trained state-sponsored team.

The second front is a major problem, since it opens up the way for new *hybrid warfare mercenarism*; just as the Iga and Koka *shinobi no mono* were employed as mercenaries, it also opens up the way for non-state-sponsored hybrid attacks from individuals or groups that have a cause or even just a grudge against a target, individuals, and groups who are skilled hackers that can perform similar operations as a *hybrid agent*.

In this sense, there can be three operational profiles for *hybrid agents* which mirror the three operational profiles for hybrid threats addressed in Section 2:

- Type 1 hybrid agent: an agent that belongs to a given state's intelligence agency and that is operating covertly
- Type 2 hybrid agent: an agent not linked to any intelligence agency but highly skilled in hacking and social engineering that is not operating on behalf of any state but is either a lone wolf or operating on behalf of some non-state group
- Type 3 hybrid agent: an agent not linked to any intelligence agency but that performs hybrid operations for hire

The three types of agents may coexist and constitute a major threat for countries' national security and defense; on the other hand, one may also recognize that, while constituting a threat, any state may take advantage of these three types of agents in its own operations, with particular relevance to types 1 and 3 as well as the

relevance of the tactical openings provided by the actions of type 2 agents. There is a fluid border between the three types, where agents can change their profile along the course of their activities.

The question that can be raised is: *what responses need to be implemented in terms of CI to deal with the twenty-first century hybrid agent?* The answer is somewhat complex, in the sense that the threat landscape is changing with the exponential technological revolution that greatly enhances the disruptive power of the new hybrid HUMINT, which can synergistically combine traditional with high-tech methods to become one of the most disruptive forces in the new defense and security context, but, given an identification of major targets, in particular economic and financial targets (that may become key parts of economic, financial and political warfare), there are specific responses that need to come into play with some urgency. This forms part of our final reflection on the whole chapter and is integrated in the next section, which concludes the chapter.

5. A final reflection and possible responses

Throughout the chapter we laid out the profile as well as the current and foreseeable evolution of hybrid operations and hybrid threats (Section 2). We also addressed the issue of weaponization of cyberspace, the use of AI and data science, and the threat patterns of *cyber psychological operations* in the context of hybrid operations (Section 3), and, in Section 4, we introduced the concept of *hybrid agent*, evaluating its overall pattern of activity and threat to countries' defense and security.

Some major points need to be highlighted, when dealing with *hybrid threats*, namely:

- Operations on the virtual space can have physical consequences, even in the cases where the operation does not directly disrupt physical systems.

- Related to the previous point, behavioral hacking is a major component of *cyops* and can take advantage of the impact of fake contents, propaganda, disinformation, as well as strategic leaks of critical data, in order to affect people's behaviors.

- *Gamification* and implementation of viral online *challenges* can support *terror games* that may gain a form of digital continuity, such that the game can be recovered anytime, even after the arrest of key individuals and groups, being perpetuated independently of what happens to the initiators of these *terror games*, and can be kept going by *bots* as well as by people willing to play the game, taking advantage of the dynamics between AIs and social media.

- A new form of operative, the *hybrid agent*, leads to an amplification of the synergy between HUMINT, SIGINT, and OSINT with HUMINT playing the nexus role, in which an undercover agent takes advantage of the physical presence on any given organization and employs classical HUMINT strategies and tactics along with hacking and *cyops* to enable and enhance the disruptive potential of well-orchestrated *hybrid campaigns*.

These are some major points that were addressed in detail in the previous sections. Now, as part of a final reflection, the question may be raised: *what to do about all this?*

From the work developed throughout the sections, one thing becomes clear: there is an urgent need for the strategic integration in key state and private

organizations, including the defense and security community, of a concept of *hybrid resilience*, of which *cyber resilience* is just an aspect. In this sense, in what regards CYBERINT [28], its focus needs to address the profile of cyber-threats and *cyop* profiles associated with hybrid strategies, in the sense that tactical dynamics of cyberattacks may obey to the pattern needed for a given hybrid strategy, and it needs to cooperate with HUMINT/CI in order to find countermeasures against *hybrid HUMINT* operatives.

The concept of *hybrid resilience* as the ability to resist and recover from *hybrid campaigns* should be a major component of countries' national defense and security strategies.

Now, secondly, organizations should have training and a *hybrid defense and CI division* or at least subcontract specialized people in this area, covering both *cyber defense* and *cyber resilience* as well as *hybrid defense* and *resilience*.

Faced with the threat of economic, financial, and (geo) political hybrid warfare, any country's major business and financial targets should have specialized training programs and people involved in *hybrid defense strategies* and *hybrid resilience*, including CI-based defense against possible disruption from what may become the new disruptive face of HUMINT: the *hybrid HUMINT*.

It is not enough to secure the technical side of cybersecurity, and one needs to address the social and human aspect of cyber intrusion, in which people's behavior can be turned against them, including the behaviors and vulnerabilities that come from incorrect social network usage.

Campaigns in the standard media against fake contents need to be addressed, as well as large-scale educational programs that should start in schools, educating civil society on the correct usage of cyberspace, on both the positive and negative, on how people can protect themselves against cyberbullying and hybrid campaigns, and on how people should read and reflect on the contents that they read and share.

While these are some of the major changes needed to be implemented for any country's successful *national hybrid defense strategy*, there is a main point of *hybrid resilience* that was already identified in the old Chinese and Japanese classics, in particular in *Tai Kung's Six Secret Teachings* [4] and in the *Bansenshukai* [5]: without good governance there is always a fundamental vulnerability to hybrid strategies.

The three major crisis profiles that were addressed in [29] and recovered in Section 2 come out of bad governance that is unable to face crises that affect its country's people (*resilience problems*), that is totalitarian and oppressive and that enforces its rule by force or has alienated a large part of its people due to rising inequalities and widespread political, business, and financial corruption (*legitimacy problems*), or that is unable to manage its territory (*authority problems*). All these three problems open up any country to *hybrid threats* and reduce a country's *hybrid resilience*.

Author details

Carlos Pedro Gonçalves
Institute of Social and Political Sciences, University of Lisbon, Lisbon, Portugal

*Address all correspondence to: cgoncalves@iscsp.ulisboa.pt

References

[1] Atkinson C. Hybrid warfare and societal resilience: Implications for democratic governance. Information and Security: An International Journal. 2018;**39**:63-76. DOI: 10.11610/isij.3906

[2] Nikolic N. Connecting conflict concepts: Hybrid warfare and warden's rings. Information and Security: An International Journal. 2018;**41**:21-34. DOI: 10.11610/isij.4102

[3] Treverton GF. The intelligence challenges of hybrid threats: Focus on cyber and virtual realm. Sweden. Center for Asymmetric Threat Studies. 2018. 36p. ISBN: 978-91-86137-75-5. Available from: http://fhs.diva-portal.org/smash/get/diva2:1250560/FULLTEXT01.pdf [Accessed: 04 June 2019]

[4] Sawyer RD. The Seven Military Classics of Ancient China. United States: Basic Books; 2007. 568 p. ISBN:0-8133-1228-0

[5] Cummins A, Minami Y. The Book of Ninja: The First Complete Translation of the Bansenshukai, Japan's Premier Ninja Manual. London: Watkins Publishing; 2013. 512 p. ISBN: 978-1-78028-493-4

[6] Cummins A, Minami Y. True Path of the Ninja: The Definitive Translation of the Shoninki. Singapore: Tuttle; 2011. 191 p. ISBN: 978-4-8053-1114-1

[7] Cummins A, Minami Y. The Secret Traditions of the Shinobi: Hattori Hanzo's Shinobi Hiden and Other Ninja Scrolls. Berkeley: Blue Snake Books; 2012. 194 p. ISBN: 978-1-58394-435-6

[8] Machiavelli N. Art of War. Chicago: The University of Chicago Press; 2003. 262 p. ISBN: 0-226-50040-3

[9] Chekinov SG, Bogdanov SA. The nature and content of a new-generation war. Military Thought: A Russian Journal of Military Theory and Strategy. 2013;**4**:12-23

[10] Normak M. How States Use Non-State Actors: A Modus Operandi for Covert State Subversion and Malign Networks. The European Centre of Excellence for Countering Hybrid Threats. 2019. Available from: https://www.hybridcoe.fi/wp-content/uploads/2019/04/HybridCoE_SA_Non-state-Actors_RGB_NEW.pdf [Accessed: 24 April 2019]

[11] Raugh DL. Is the hybrid threat a true threat? Journal of Strategic Security. 2016;**9**:1-13. DOI: 10.5038/1944-0472.9.2.1507

[12] Vosoughi S, Roy D, Aral S. The spread of true and false news online. Science. 2018;**359**:1146-1151. DOI: 10.1126/science.aap9559

[13] Nisbet EC, Kamenchuk O. The psychology of state-sponsored disinformation campaigns and implications for public diplomacy. The Hague Journal of Diplomacy. 2019;**14**(1-2):65-82. DOI: 10.1163/1871191X-11411019

[14] Nemr C, Gangware W. Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age. 2019. Park Advisors. Available from: https://www.state.gov/documents/organization/290985.pdf [Accessed: 28 April 2019]

[15] Howard F, Onur K. Poisoned Search Results: How Hackers have Automated Search Engine Poisoning Attacks to Distribute Malware. SophosLabs Technical Paper. 2010. Available from: https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophosseoinsights.pdf [Accessed: 28 April 2019]

[16] Leontiadis N, Moore T, Christin N. A nearly four-year longitudinal study of

search-engine poisoning. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM; 2014. pp. 930-941. DOI: 10.1145/2660267.2660332

[17] Guess A, Nyhan B, Reifler J. Selective Exposure to Misinformation: Evidence from the Consumption of Fake News During the 2016 U.S. Presidential Campaign. European Research Council. 2016. Available from: https://www.dartmouth.edu/~nyhan/fake-news-2016.pdf [Accessed: 06 May 2019]

[18] Hans K, Ahuja L, Muttoo SK. Performance evaluation of neural network training algorithms in redirection spam detection. In: Panigrahi B, Hoda M, Sharma V, Goel S, editors. Nature Inspired Computing. Advances in Intelligent Systems and Computing. Vol. 652. Singapore: Springer; 2018. pp. 177-183. DOI: 10.1007/978-981-10-6747-1_20

[19] Lupariello F, Curti SM, Coppo E, Racalbuto SS, Di Vella G. Self-harm risk among adolescents and the phenomenon of the "Blue Whale challenge": Case series and review of the literature. Journal of Forensic Sciences. 2019;**64**(2):638-642. DOI: 10.1111/1556-4029.13880

[20] Khattar A, Dabas K, Gupta K, Chopra S, Kumaraguru P. White or Blue, the Whale gets its Vengeance: A Social Media Analysis of the Blue Whale Challenge. 2018. Available from: https://arxiv.org/pdf/1801.05588.pdf [Accessed: 10 May 2019]

[21] Foucault M. Microphysics of Power (Microfísica do Poder). Edições Graal: Brazil; 1979. 295 p. ISBN: 9788570380746

[22] O'Neil C. Weapons of Math Destruction—How Big Data Increases Inequality and Threatens Democracy. New York: Crown; 2016. 259 p. ISBN:978-0-553-41881-1

[23] Błasik P. Social networks and personal security. Scientific Journal of Bielsko-Biala School of Finance and Law. 2018;**22**(3):13-16. DOI: 10.19192/2543-411X-3

[24] INTelligence: Human Intelligence. 2010. Available from: https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html [Accessed: 29 May 2019]

[25] Cummins A. In Search of the Ninja: The Historical Truth of Ninjutsu. The UK: The History Press; 2012. 239 p. ISBN: 978-0-7524-8093-0

[26] Cummins A, Minami Y. Iga and Koka Ninja Skills: The Secret Shinobi Scrolls of Chikamatsu Shigenori, Including a Commentary on Sun Tzu's 'Use of Spies' in The Art of War. UK: The History Press; 2014. 189 p. ISBN: 978-0-7509-5664-2

[27] Hughes-Wilson J. On Intelligence. UK: Constable; 2016. 528 p. ISBN: 978-1-47211-354-2

[28] Clark RM, Oleson PC. Cyber intelligence. Intelligencer: Journal of U.S. Intelligence Studies. 2018;**24**(3): 11-23 Available from: https://www.afio.com/publications/CLARK_OLESON_Pages_from_Vol24_No3_AFIO_INTEL_Winter_2018-19_FINAL.pdf [Accessed: 04 June 2019]

[29] Margolis JE. Estimating state instability. Studies in Intelligence. 2012;**56**(1):13-24. Available from: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-1/pdfs-vol-56.-no.-1/Estimating%20State%20Instability%20-Extracts-Mar12-20Apr12.pdf [Accessed: 24 April 2019]