6

NovaFeed – Modern War in the Office

Calvin Chrustie & Adrian Borbély

This case describes the plight of a news media company, based in a Western liberal democratic country (Federatio) which employs immigrants from two countries, Agraria and Voracia. When full-scale war breaks out between Agraria and Voracia, the company decides not to relay news articles from Voracia news outlets suspected of propaganda. Soon afterwards, it is hit with a ransomware attack by hackers originating from Voracia. All activities are halted, a multi-million ransom is demanded, and the staff's personnel records are compromised.

The case is particularly interesting in showing how a private enterprise may be specifically targeted because of a geopolitical crisis, i.e., how kinetic and hybrid warfare may coexist.

* * *

Keywords: Hybrid warfare – Cyber criminality – Hacking – Disinformation – Kinetic warfare – Espionage.

NOVAFEED – MODERN WAR IN THE OFFICE

Calvin Chrustie & Adrian Borbély

A few months ago, the country of Voracia has launched a major invasion of one of its neighbors, Agraria, following longstanding border disputes. Despite its relative smaller size, Agraria has been resisting, in the face of full-fledged kinetic war waged by Voracia, which is conducting bombings, airstrikes, naval operations, and army movements. Liberal democracies, such as Federatio, have pledged to support Agraria in the form of armament delivery and economic support; however, they have so far refused to get involved on the battlefield, fearing the consequences of an all-out war with Voracia.

The region has been characterized, over history, by important population movements, both before and after formal borders were drawn to demarcate Nation-States. Consequently, people who are now citizens of a particular country often have family ties in neighboring countries (e.g., Agrarian people have family in Voracia, and vice versa).

In this context, NovaFeed Inc. is a Federatian tech firm which specializes in the distribution of online news stories through a digital platform on smartphones. Wherever they are, users of the NovaFeed app may access news sources from around the world and select the articles they are interested in simply by swiping. An artificial intelligence engine then analyzes the user choices to provide more accurate suggestions in the future. The longer the user uses the app, the better the content suggestions provided to him.

While the company is incorporated in Federatio and based in its capital city, its CEO is the son of Voracian immigrants, and most of its about 600 employees are of Agrarian or Voracian descent, some of them first-generation immigrants (e.g., people who came to Federatio to attend college), others stemming from families that have been emigrating to Federatio in waves over the last century. The company has contracts with 2,500 media outlets around the world, who often report on current affairs, including the war in Agraria.

Within days of the war breaking out, the company decided that, for reputational and ethical reasons, they would terminate their contracts with half a dozen Voracian media, as it was being reported that the Voracian Government and its armed forces were using those media to spread fake news for misinformation and disinformation purposes. Such fake news included minimizing civilian casualties, attempting to rebut stories of human rights abuses, and propaganda in support of Voracia's aggressive military action.

Several days after the decision was implemented, first thing one morning the C-Suite staff and legal counsel were called to the boardroom for an urgent meeting. The CEO briefed them that the night before, they had been hit with a cyberattack that affected their entire system and forced them to interrupt their services. Their 2,500 global clients could no longer share their news stories on the platform. The system shutdown was accompanied by a ransom demand for 5 million in cryptocurrency. The cyber hackers identified themselves as belonging to an infamous Voracian cyber hacking organization, who coincidentally, just days before, had publicly said they aligned with the Voracian military.

The attack and ransom demand led to the following immediate consequences:

- By freezing all NovaFeed's systems, the hackers severed some of the world's largest national news outlets' access to their global audience. It so happened that many of these news outlets were reporting on the Voracian invasion, mostly from the perspective of liberal democratic societies. The phones in the office were ringing non-stop.
- Within 12 hours, some of these clients had terminated their contracts, making their articles no longer available to the public through the NovaFeed app.
- Users who were interested in those sources were moving to competing providers.
- It also rapidly became obvious that the hackers had accessed and hijacked the company's employees' personal data.

Since half the staff members were of Voracian descent, and the other half of Agrarian origin, often with direct family ties back in their countries of origin, tensions in the office seemed to be rapidly escalating between the two camps. The international context appeared to be imported within the once harmonious company: resentment was growing, and the personnel started voicing strong concerns.

The C-Suite agreed they needed external support, both to secure the company's IT systems and to manage the crisis. But whom to call?

- Within the first several hours, disagreements emerged regarding whether – or not – to engage with law enforcement. Although they felt they needed help from the authorities, there were risks attached to such a move, especially in terms of discretion and company reputation. Plus, the C-Suite members were not clear as to what exactly police personnel could do, without taking control over the company (and circumventing the Board itself).
- A crisis management consultant was hired to provide expertise and an independent perspective on the issue.

- Efforts were made to hire specialized legal counsel, law professionals experienced with such cyber incidents. However, many refused to get involved, fearing they would then themselves become targets of Voracian hackers.

Within the C-Suite, disagreements rapidly grew on whether to be transparent with employees regarding the fact that their personal data may be in the hands of Voracian hackers aligned with the Voracian military and intelligence services. Employees of both Voracian and Agrarian descent could be directly exposed.

The C-Suite is particularly concerned with the fact that for the previous holiday party, HR put together what was then a fun teambuilding exercise. They sent a survey to all staff members asking them where they have family roots (where their grandparents were born, where their family's favored vacation places were, etc.), so that an interactive map could be created, enabling employees to identify with whom they may be related, or share a common history. All the data used to set up this map were in the HR database that has been hacked, which now places the personnel's relatives back in the region also at risk.

The C-Suite immediately considered the option of paying the hackers. However, concerns were raised that paying the ransom to get the business up and running could be considered an illegal transaction. Indeed, such a money transfer may very well violate international sanctions against Voracia, its government and wealthy supporters. It may also violate other Federatian or international illicit finance laws.

The crisis management consultant raised the fact that intelligence suggests that, even if the company did pay the ransom, there was a high probability their systems would not be returned to functioning order, or that they will be extorted again. Furthermore, there was no guarantee that the staff's personal data would be retrieved and not sold to a third party or used by Voracian intelligence services to target individuals working for the company – or related to them.

On day 3, the CEO made the executive decision to pay the ransom. His reasoning was that this was less harmful than seeing dozens of his company's clients vanish daily, which equated to millions in lost revenue.

Possible questions for all audiences

1) What elements seem to indicate that we are in a hybrid warfare situation? What are the different warfare tactics at play in this scenario? Discuss the link between kinetic and hybrid warfare mechanisms.
2) Draw a stakeholder map of all concerned actors, with their relationships to one another. Such a map is a graphic representation of all actors, with arrows between them signifying opposition or support. Identify the interests and values of the main actors.
3) NovaFeed Inc. is a private company, not a military operation; yet it became a target due to its business and the way it is staffed. Despite these elements, it seems ill-prepared for such a scenario. How do you explain this? What could they have done to prepare?
4) Regarding the decision to exclude Voracian outlets accused of propaganda: should the Board have included the staff in the decision-making process? Should all have raised the security level in anticipation of a likely attack?
5) Should the company have been transparent with its personnel about the data theft? Discuss the pros and cons of the decision to communicate or retain information.
6) What could the hackers do with the stolen data? At first sight, this attack has to do with economic coercion or subversion (extortion and/or destruction of the NovaFeed business). But the data could also be used for transnational suppression (harassment of people that remained in the war-torn region) and/or espionage (using these people to blackmail and recruit new assets in Federatio). What other possible uses are there?
7) International conflicts are sometimes "imported" into an organization's personnel. As a business manager, what steps can you take to prevent this or deal with it?
8) Should the company pay the ransom? Please address the pros and cons of both alternatives, before justifying your decision.

Possible specific questions for lawyers and law students

1) If you were the lawyer hired by NovaFeed, what would you advise your client to do and why?
2) Imagine that NovaFeed pays the ransom, without consulting their lawyers ahead of time. In other words, lawyers discover this after the fact. What risks do the company and its CEO face?
3) An employee of NovaFeed consults you, as a lawyer, regarding personal data being stolen by a hacker group linked with an adversary nation. Is the employee entitled to compensation? What would you advise in terms of litigation and negotiation? What would be the drawbacks of such a claim?
4) Assume the company's contracts with news generators include a typical *force majeure* clause. What risks does NovaFeed face from their clients? Are we here in a *force majeure* scenario that would prevent clients from asking for compensation? More generally, apply the criteria for *force majeure* to hybrid warfare scenarios.
5) Do you understand the decision of several law firms not to get involved in the situation? Does this infringe on your jurisdiction's attorney-ethics rules? In other words, what are the reasons why a firm may refuse to advise and/or defend clients? Are ethical codes up to date regarding such international risks?
6) As a lawyer advising or defending a client who is a target of hybrid warfare, do you consider yourself at risk? Would you notify your insurer if put in such a situation?