Letter From a Venezuelan Jail

By Leopoldo López

The National Assembly of Venezuela, a supposedly democratic body, was recently seized by a group of soldiers who were acting as the front for an illegal, armed force led by one of the country’s ruling elite. The scene was ugly. The National Assembly was hosting an emergency session of the constituent assembly. The government, which has been in power for more than a decade, has systematically institutionalized one of the world’s most authoritarian and repressive regimes.

This is not the first time in Venezuela that this group of soldiers has acted under the orders of the government. In recent years, the government has repeatedly mobilized the armed forces to maintain control over the country, which has been wracked by violence, poverty, and food shortages.

In the beginning, the government’s actions were motivated by a desire to suppress opposition movements and prevent them from gaining influence. However, as the situation worsened, the government increasingly relied on violence and repression to maintain its grip on power.

The government’s actions have placed the country on the brink of a humanitarian crisis. According to international organizations, millions of people are facing food shortages and accessing basic necessities is becoming increasingly difficult.

The government has repeatedly denied reports of human rights abuses and has steadfastly refused to engage in meaningful dialogue with opposition leaders and civil society groups. Instead, it has continued to use violence and intimidation to silence opposition voices.

In a climate of fear and intimidation, it is difficult to imagine that meaningful political change will be achieved. The government’s actions have only served to reinforce the country’s isolation and further isolate it from the international community.

The government’s actions are a clear violation of international law and have grave consequences for the people of Venezuela. The international community must take action to hold the government accountable and ensure that the country’s human rights are respected and protected.
A devastating assault like this could stop organisations including critical organisations such as healthcare from operating, literally costing lives. As the likelihood of a major cyber-event increases, it’s important to be prepared. From a business and organisational perspective, the only way to stop or limit the risk of a cyber pandemic is by embedding a culture of cyber awareness into people’s work and personal lives. It requires education and training, which should be updated regularly to reflect the threats all organisations face from malicious actors including nation states. Stopping the Next Cyberassault. Dec 2014. Mike Rogers. Mike Rogers, “Stopping the Next Cyberassault,” The Wall Street Journal, December 25, 2014. (http://www.wsj.com/articles/ mike-rogers-stopping-thenext-cyberassault-1419543945). NY Bank Regulator Targets Cyber Threat. Oct 2014. Stopping the Next Cyberassault. Congress needs to expand private-sector access to classified intelligence about threats. By Mike Rogers. FireEye’s report notes that FIN4 has hacked into nearly 100 publicly traded companies and collected sensitive insider financial information in what is probably an attempt to manipulate the stock market for profit. FIN4 uses sophisticated techniques, has native-English language skills, and demonstrates detailed knowledge of corporate practices and financial markets. Cyber financial crimes are not new, but FIN4 shows that the threat has grown and evolved dramatically. The Sony hack and FIN4 will not be isolated cases. The first generation of cyber conflict kicked off shortly after the dawn of the internet (then called ARPANET) in the mid-1980s. The primary actors were the old Cold War superpowers, sometimes assisted by their respective NATO and Warsaw Pact allies. The phase continued through the late 1990s, as they targeted each other’s military and government networks for the purpose of traditional state-on-state espionage. The newly created cyber domain allowed them to augment decades-old signal-intelligence. The SolarWinds cyber-espionage campaign was a primary concern. To maximise the impact they have combined response to this with sanctions over election interference and other issues. Diplomatic expulsions and sanctions against individuals will largely be shrugged off by Moscow as expected. The financial sanctions regarding Russian sovereign debt are a step-up though. The US has also published a huge amount of detail about Russian intelligence activities ranging from front companies involved in spreading disinformation to Russian tech companies allegedly supporting its intelligence services. The