30 April 2021

An Analytic Intelligence Wire Prepared by The Students of Embry-Riddle Aeronautical University

Issue 383
Of Eagle Eye Intelligence

Authors
Savannah Grace Riddles
Amalie Hansen
Austin Johnson

Source: Reuters

30 April 2021

Issue 383
Of Eagle Eye Intelligence

In This Issue

EUROPEAN UNION: AstraZeneca Vaccine Likely to Result in Public Distrust and Delayed Immunity

Summary: Recent controversy surrounding AstraZeneca and its COVID-19 vaccine complicate vaccine rollout in the European Union (EU). The dispute between the company and EU member nations will likely result in decreased public trust in vaccines and delayed immunity across the continent.

Background: On 27 August 2020, the EU and British-Swedish multinational pharmaceutical company AstraZeneca entered a contract to secure a COVID-19 vaccine for EU member nations. AstraZeneca faced several setbacks across the globe, including doubts to whether it protects against the B.1.351 South African variant of the virus. South Africa promptly halted the use of the AstraZeneca vaccine and other countries took notice when the variant started to spread. AstraZeneca failed to quickly produce the doses promised to the EU which led to increasing tensions between the company and member nations. EU citizens grew increasingly restless from the continued COVID-19 restrictions and the conflicting information about vaccine efficacy and safety, leading to protests in favor of lifted quarantine and mask mandates. World leaders tried to remedy some of the public perception issues by getting the AstraZeneca vaccine themselves, including Boris Johnson, Justin Trudeau, and Angela Merkel.

Legal Repercussions of Vaccine Shortage: Legal disputes between nations and their respective vaccine manufacturers may result in an ongoing battle, at least until a vast majority of the population receives the vaccine. The EU claims that AstraZeneca fell short of its promises to provide 100 million doses in the first quarter of their contract. AstraZeneca sent only 30% of contracted doses to EU member nations in that time frame, although AstraZeneca claims that the contract only requires it to make its “best reasonable efforts” to follow through. In the wake of this ongoing contact dispute, six EU diplomats claim that the EU plans to sue AstraZeneca in attempt to force the supply of the remaining contracted doses. The EU will likely face a public perception issue regarding the vaccine if it does enforce the supply of more doses. EU citizens will almost certainly prefer an alternative vaccine. According to Politico, most EU nations seem interested in joining the lawsuit, but each country will decide individually whether to participate. Some ambassadors spoke up after a European Commission meeting on the matter and shared hesitations about the suit because they worry that the EU cannot enforce a ruling in its favor. The lawsuit may do more harm than good. If the suit impacts funding or manufacturing at AstraZeneca, it may not follow through on the contract anyway. Some EU nations may feel pressured to join the lawsuit if more powerful EU nations participate, regardless of whether the suit will benefit the country.

Fears About Blood Clotting: Blood clotting as a side effect may become a more politicized issue after multiple vaccines presented a risk of clots. The EU and the United Kingdom recently reported occurrences of severe blood clotting as a side effect of the AstraZeneca vaccine. A recent Norwegian study concluded that the risk of dying from the AstraZeneca vaccine exceeds the risk of dying from COVID-19. More countries worldwide use the AstraZeneca vaccine than any others, mainly due to its cheap cost and less restrictive storage requirements. Many EU nations paused the use of the vaccine in response to the blood clot reports, and Denmark halted the use of the vaccine completely. EU citizens may choose to delay their vaccinations until the EU supplies more data, which would most likely contribute to the spread of COVID-19 in Europe at a time of year when the tourism industry profits most. Individual member states get to

decide individually on how to handle future doses. If EU member nations stop the use of the AstraZeneca vaccine, they may instead donate it to poorer nations and refugee communities, contributing to a global disparity in healthcare and immunizations.

Outlook and Implications: A lawsuit between AstraZeneca and the EU will likely only further politicize the vaccine distribution efforts across Europe and around the world. Vaccine efforts in the EU will most likely decelerate in fears of making similar mistakes with pharmaceutical companies in the future. After the drawn-out dispute between the EU and AstraZeneca, it proves highly unlikely that any other country will approve the vaccine for emergency use. The continued, highly publicized issues surrounding the AstraZeneca vaccine will likely add to the public's hesitation to trust immunizations for COVID-19 or other preventable diseases. The EU may exclude AstraZeneca from consideration in vaccine developments for future global health concerns. The company may not survive a scandal this large and impactful, and even if it did, the company would likely benefit from a merger, rebranding, or a shift away from vaccine production.

[Savannah Grace Riddles]

UNITED KINGDOM: New Cyber Force Likely to Inspire Businesses to Invest in Cyber

Summary: London's announcement of the new National Cyber Force will most likely inspire companies to increase their cyber security budget and dedicate more resources to the education of employees as cybercrime will almost certainly continue to remain an issue post pandemic. Proper education would most likely help companies decrease the chances of suffering expensive attacks, though it will most likely not stop attacks from happening.

Background: The number of cybercrimes reported by businesses increased as the COVID-19 pandemic hit. This trend escalated as the pandemic forced several companies to shift employees to working remotely. The rapid shift in the location of the workforce, while also making many additional services available to customers online, allowed hackers to easily detect vulnerabilities in companies' newly changed IT infrastructures. Not only have the employee's remote connection gotten more unsecure, but the cyber criminals behind the attacks also proved that their skill levels continue to increase immensely. Through the course of the pandemic, hackers managed to quickly adapt to the new circumstances and exploited the fears of their victims through ransomware and highly sophisticated phishing attacks. London recognizes that the trend will not decrease unless it meets resistance. Therefore, it announced an investment of $22 billion to a new National Cyber Force (NCF).

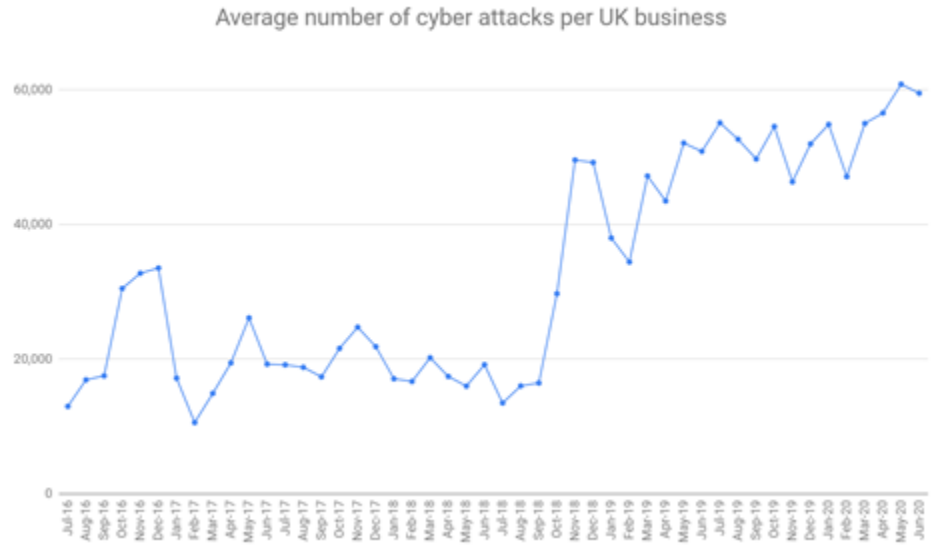

Figure 1: Average number of cyber-attacks per UK business July 2016 - June 2020

Cybercrime Statistics: The increase in cybercrime will most likely continue to target individuals and business after the pandemic comes to an end. Cybercrime flourished as many individuals struggled to become oriented with the changes that the pandemic brought on as indicated by the spike in attacks in the period March to April 2020 in Figure 1. In the last two quarters of 2020 reports found 648 threats per minute, COVID-19-related cyber-attack detections increased by 240%, and PowerShell threats climbed to 208% above normal, according to a threat

report conducted by McAfee. On average, one in five of UK businesses experienced a cyber-attack. The actors used the pandemic panic to their advantage and quickly adapted to the new and expanded playing field. Workers working remotely opened the possibility of hackers exploiting their unsecure home devices, networks, and VPNs. As a result, UK businesses experienced an average of 177,000 attacks in the span of 3 months, which translates to about one attack every 45 seconds, according to Beaming. The upward trend of cybercrime will almost certainly continue and will likely take advantage of the momentum built throughout the pandemic.

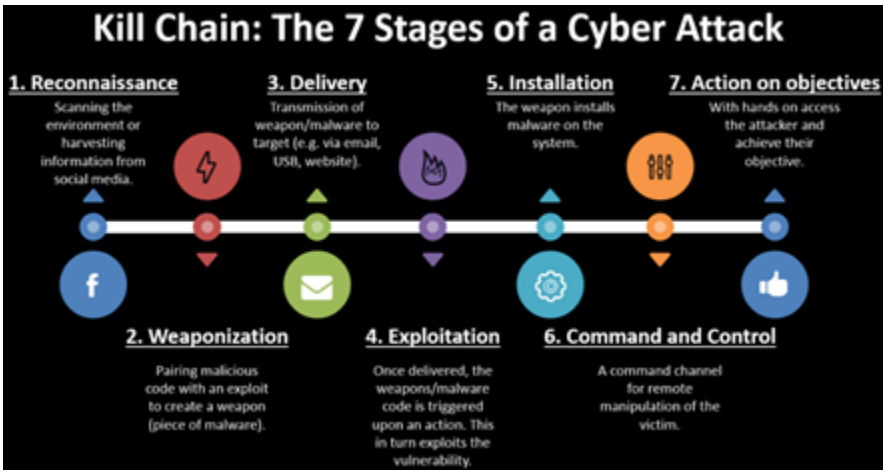

Figure 2: The usual steps taken in most cyber-attacks.

Education Plays Key Role in Security: Most major businesses will most likely increase their budget for cyber security as threats of attack almost certainly continue. Once a business experiences a successful cyber-attack like a ransomware attack that freezes access to their system, or a malware attack that prohibits their software from working on the host and client side, most suffer millions in monetary loss and end up losing even more on asset and recovery costs. As a result of the recent trends, a majority of the UK's CEOs reportedly chose to prioritize cyber during the next three years, according to the 24h annual UK CEO Survey. Many businesses continuously recognize that they need to secure not only the vulnerabilities of their IT but also the ones found within the organization. Good cybersecurity measures start with the education of the employees in strategies such as anti-phishing, including how to recognize malicious emails, which typically get sent out by the hacker as step five in their attack strategy as seen in figure 2, or in using safer login credentials such as two-factor authentication and unique passwords.

National Cyber Force: London's creation of the NCF will most likely inspire more businesses to follow its lead and implement better cyber security protection measures. The task force, which Prime Minister Boris Johnson announced on 19 November 2020, will consist of personnel from the Secret Intelligence Service, Intelligence, and the Defense Science and Technology Laboratory. The force contributes to London's plan to help prevent the internet from further turning into a global platform for serious crimes. This act greatly impacted the rest of the UK as

it proves the danger of cyber but also the worth of protecting against it, which will likely add to businesses desire to implement strong cyber security protocols and procedures.

Outlook and Implications: London dedicating more money, assets, and personnel to upgrading the national policy level of cyber security will almost certainly create a positive impact and inspire more business, and possibly even other countries, to follow its lead and do the same. A stronger foundation of cyber security will almost certainly help companies suffer less fatal cyber-attacks that could end in them going out of business. The increase of the cyber budget will almost certainly send a strong signal to the hackers and could possibly cause the trend of attacks to decrease, although it will likely not stop all attacks from happening. Educating employees could prevent additional attacks as employees would almost certainly gain knowledge on how to identify malicious emails and malware that could potentially pose risks to the organization.

[Amalie Hansen]

MEXICO: Cartel Violence may Prompt Call for International Intervention

Summary: The Jalisco New Generation Cartel (CJNG) continues to attempt to exert control over rural and urban areas in the state of Jalisco through increasingly violent methods. To curb the violence and stop CJNG, Mexico City may seek international intervention to aid its efforts.

Background: Over the last few years, Jalisco experienced a violent upwards trend in cartel crime. A highly militarized cartel, the CJNG cartel is known for an extremely violent tendency for creating mass graves, hangings, and other acts of violence. CJNG is responsible for fighting rival cartels, police, and military forces; these fights have mainly occurred in rural locations but recently the violence made its way into Guadalajara and many other major cities. Local law enforcement and military forces continue to struggle to combat CJNG's expansion.

Figure 1: CJNG armored vehicles driving through Guadalajara (Mexico News Daily 2021).

Increasing Violence: On 23 March, police found the body of an ex-CJNG lieutenant with a note that translated to "the traitor", indicating CJNG's increasing boldness in its displays of violence and the growing potential for future attacks. CJNG recently increased violent attacks against aggressors in urban Jalisco. The fighting involves the cartel, police, military, and civilian militia. When s CJNG moves into a new region to operate drug trafficking, violence associated with its illegal endeavors frequently follows. On 13 February, police uncovered 18 trash bags filled with severed body parts found outside of Guadalajara holding the cartel responsible. Police linked the unidentified victims to the ongoing drug war in Jalisco. The evidence suggests the victims are part of a larger network of mass graves that CJNG uses to dispose of anyone that interferes. Police estimate that there are over 62,000 people reported missing in connection to the drug war. The CJNG continues to amass a larger arsenal to combat the police and military. This includes the use of machine guns, rocket launchers, grenades, sniper rifles, and other assault weapons

against aggressors. Mexico City considers CJNG a paramilitary force due to the violence and arsenal it employs.

Territorial Pseudo Governing: CJNG exerts control over rural towns, a likely indication of its increasing power and influence in the region. If the town does not comply, the cartel kills the townspeople and cuts off the town from the outside world. When these towns comply, the cartel runs every aspect of the town. This instills fear in rural citizens and places CJNG into a governing position. Cartels including CJNG worked to exploit the COVID-19 pandemic through adopting the roles of legitimate governments. In rural areas, the cartels enforce mask mandates, social distancing, and hand out medical aid to those in need. CJNG will likely continue to work to capitalize on the opportunity to present itself legitimately in the regions in controls, further diminishing the authority of legitimate government officials.

Outlook and Implications: If CJNG is successful in controlling a large urban area, it can potentially legitimize itself and instill a pseudo-government. The success of exerting control over rural towns may embolden CJNG to attempt to exert control over more urban areas. Such an attempt would almost certainly result in increased violence between CJNG and law enforcement. Increased violence will almost certainly negatively impact the lives of citizens in impacted areas, who may in turn call for Mexico City to take stronger action. Following the continuous growth of CJNG and with previous failures to contain the cartel, it remains unlikely that law enforcement could successfully stave off a large-scale attack on an urban center. Facing potential pressure from citizens and the threat of increased violence, Mexico City may request foreign military aid to help contain CJNG before conflict escalates into urbanized warfare in Jalisco. Mexico City may view international intervention in the conflict as the best option should domestic forces remain unable to contain the cartel.

[Austin L. Johnson]

About GSIS

Embry-Riddle Aeronautical University's (ERAU) Bachelor of Science in Global Security & Intelligence Studies (GSIS) degree program at our Prescott Campus blends both academic and professional studies to equip students with the knowledge and skills necessary to become future leaders in intelligence, security, and law enforcement. The program provides students with a sound foundation in the liberal arts, including international relations, foreign languages and cultures, international law, foreign policy, political and military history, and other essential topics.

About EE

Eagle Eye Intelligence (EE) is an intelligence and research organization led by the students of the GSIS program at ERAU in Prescott, Arizona.

Dr. Philip E. Jones founded EE and Embry-Riddle's GSIS program in 2002, following a career with the Central Intelligence Agency and consulting work in international development and global security. Currently, Professor Dale R. Avery, a former career intelligence analyst at the Central Intelligence Agency and Office of the Director of National Intelligence, serves as EE's faculty advisor.

EE strives to provide actionable intelligence and analysis to its customers during the academic year. We are driven by a number of goals – continuous development, nonpartisanship, interdisciplinary studies, global awareness, and professionalism.

EE does not cite sources in the final publication; however, we log every source we use in our research and are happy to share them upon request. The official EE Source Database is available on our website's resources page for a general overview of our sourcing methods.

The views expressed in this publication are those of the authors, and do not represent the position Embry-Riddle Aeronautical University or the College of Security and Intelligence.

Alli McIntyre, a junior in the GSIS program, currently serves as EE's Editor in Chief. For questions or comments, contact the team at editorsee@gmail.com or Professor Avery at 928.777.4708.

Eagle Eye Intelligence
3700 Willow Creek Rd.
Prescott, AZ 86301
eagleeyeintel.com