# NOTIONAL EXERCISE MATERIAL FOR EDUCATIONAL PURPOSES ONLY JLASS-SP AY2018 WORLD SUMMARY

the water treatment facility led to contamination of the base's water supply causing infection among nearly half of the base's population. The U.S. CAOC was non-mission capable for 96 hours at the end of the attack. The United States has not been able to attribute these actions and no organization has claimed responsibility.

Further, although significant measures are in place to secure the U.S. transportation system infrastructure, the telecommunications system, energy production and distribution systems, and water supply infrastructure remain prime cyber targets for U.S. adversaries. In some respects, cyber warfare has evened the playing field for terrorist groups and developing nations, as they can field an equally effective cyber capability as established states with robust military and security systems.

Over the years, the development of cyber "weaponry" has seen exponential growth, both in sophistication and potential to harm. Western governments have all reported incidents concerning the insertion of erroneous or misleading information into official websites intended to confuse citizens and create mistrust. Governments are not alone in suffering these information attacks. A handful of banks have also disclosed events where attackers altered checking account balances of hundreds of depositors. These malicious events have not resulted in a kinetic conflict, but ordinary citizens and businesses are panicked as they lose faith in the security of information networks. Politically, this insecurity has manifested in attempt to influence the outcome of elections, particularly in weaker nations that make up regional coalitions favorable to U.S. and European interests.

#### Zbellion

In the mid-2020s, the age demographic known as Generation Z, or Gen Z, began hitting their thirties. Like the Millennials who preceded them, Gen Z were characterized as even more comfortable – if not dependent upon – technology in nearly every aspect of their lives. Social scientists frequently characterize Gen Z as having grown up with cell phone and internet usage from a very young age, and interacting on social media websites for a significant portion of their socializing. Image and video-intensive media are more popular among this group than textual narratives, and many Gen Z self-identify by the social media communities to which they belong.

Both the September 11 terrorist attacks and the Great Recession greatly influenced the attitudes of this generation in the United States, and resulted in a feeling of unsettlement and insecurity among Gen Z. Although Millennials experienced these events during their coming of age, Gen Z lived through them as part of their childhood, affecting their realism and world-view. Although many Gen Z sought to avoid the financial stresses experienced by their parents, many found themselves stuck with excessive college debt when they discovered employment options did not meet their expectations. Gen Z are often described as seeking independence and opportunity but are also among the least likely to believe there is such a thing as the "American Dream," and that "the system is rigged" against them. Frequently seeing themselves as agents for social change, they crave fulfillment and excitement in their job to help "move the world forward." Despite the technological proficiency they possess, Gen Z actually prefer person-to-person contact as opposed to online interaction. They describe themselves as being involved in their virtual and physical communities, and as having rejected excessive consumerism.

## NOTIONAL EXERCISE MATERIAL FOR EDUCATIONAL PURPOSES ONLY JLASS-SP AY2018 WORLD SUMMARY

In early 2025, a group identifying itself as "Zbellion" gained traction on the Dark Web. Zbellion capitalized on the fears and insecurities of Gen Z, and called for a global cyber campaign to expose injustice and corruption and to support various causes it deemed beneficial. It appears that Zbellion initially formed in small groups at parks, rallies, protests and coffee shops, and grew rapidly by promoting an agenda, which targets corporations, financial institutions, and political and non-profit organizations that support "the establishment." Recruitment appears focused in large cities via face-to-face contact, providing initial instructions for accessing Zbellion websites. These websites provide target lists (to include data needed for identity and credit card theft), payloads, and exploits to activists. Zbellion uses software programs to route any proceeds into laundering programs that ultimately convert national currencies into Bitcoin and make "small, below the threshold donations" to "worthy recipients" and, if Zbellion members claim financial need, to the member who conducted the attack. Zbellion "leadership" assures its members that their cybercrimes are "ultimately justifiable" and untraceable, and that it selects its targets and beneficiaries based on secure polling of "network delegates."

Zbellion provides its members with sophisticated adaptations of the latest malware, making it difficult for cyber security programs to keep pace with the threat. Computer Network Defense (CND) analysis indicates Zbellion appears to have originated in Seattle and spread rapidly to New York City, Washington DC, Los Angeles, Las Vegas, and Austin. Today, Zbellion activities has been noted in Vancouver, Toronto, most major European cities, St. Petersburg, Istanbul, Amman, Dubai, Cairo, Tunis, Rabat, Lagos, Nairobi, Johannesburg, New Delhi, Lahore, Tokyo, Osaka, Manila, Jakarta, Hanoi, Shanghai, Beijing, Taipei, Seoul, Rio de Janeiro, Bogota, Panama City, Havana, and Mexico City.

#### **Military Conflicts**

In addition to the constant threat of terrorism, world leaders remain concerned about the potential for conventional conflicts, particularly over natural resources. For example, perceived or actual water shortages could motivate state actors to take unilateral actions to assure access to adequate water flows. In the worst case, this could result in interstate conflicts if government leaders deem assured access to such resources essential for maintaining domestic stability and regime survival. However, even actions short of war could have important geopolitical consequences. Maritime security concerns provide a rationale for naval buildups and modernization efforts, such as the continued development of blue-water naval capabilities by India and China.

### **Black Market Trafficking**

Following the end of the Cold War, Transnational Criminal Organizations (TCOs) made enormous gains in the newly opened economies of the former Soviet Bloc states and Soviet clients globally). During the 1990's economic chaos in these countries produced opportunities for TCOs to open new markets in illegal drugs, weapons, WMD, technology, mineral trafficking, and human trafficking.

During the first decade of this century, Transnational Organized Crime (TOC) flourished and aspiring terrorist organizations, such as AQ and Hezbollah, mimicked their business models. This bolstered terror networks revenues and providing them new global reach through established "Black Market" shipping channels though led to confrontation with traditional TCOs with overlapping business interests. While occasionally coming into conflict, many of the TCOs