Cyber Center of Excellence

Unclassified Threat Read Book

1-15 January 2023

Prepared by: Threat Management Office
CCoE
Fort Gordon, GA 30905

POC: Threat Management Office: jeffrey.t.hardimon.civ@army.mil, kevin.m.bird.civ@army.mil
706-849-9263/9266

Cyber

1. **Cyberattack keeps Iowa's largest school district closed (AP, 10 JAN Scott McFetridge)**

   An apparent cyberattack on Iowa's largest school district has led officials to cancel classes for 30,000 students for a second day as technicians scramble to protect data and restore the computer system, the district's leader said Tuesday afternoon.

   The Des Moines school district's interim superintendent, Matt Smith, said officials received an alert Monday about a possible "cybersecurity event" that led them to cancel classes Tuesday and then to keep schools closed Wednesday. On Tuesday night, the district announced that school would reopen Thursday.

2. **1 in 5 government passwords were cracked by Interior's own hack (Federal Times, 10 Jan, Molly Weisner)**

   The Department of the Interior "hacked" itself to test how easy it would be to crack employee passwords.

   It was easier than it should've been, according to Jan. 3 report from its Office of Inspector General. In 90 minutes and with less than $15,000, the OIG's system obtained clear-text passwords for 16% of user accounts.

3. **Notorious Russian Spies Piggybacked on Other Hackers' USB Infections (Wired, 05 JAN, Andy Greenberg)**

   THE RUSSIAN CYBERESPIONAGE group known as Turla became infamous in 2008 as the hackers behind agent.btz, a virulent piece of malware that spread through US Department of Defense systems, gaining widespread access via infected USB drives plugged in by unsuspecting Pentagon staffers. Now, 15 years later, the same group appears to be trying a new twist on that trick: hijacking the USB infections of other hackers to piggyback on their infections and stealthily choose their spying targets.

4. **CYBER101: Joint Force Headquarters–Department of Defense Information Network (JFHQ-DODIN) (U.S. Cyber Command Public Affairs, 03 JAN)**

   A digital revolution in cyberspace has swept the globe over the last three decades leading to the interconnectivity of disparate nations, organizations, groups, and people across a worldwide network of information and things. This revolution has had a massive impact on everything the Department of Defense (DoD) has in its vast arsenal.

   With cyberspace an integral part of all facets of American life, the increase in interconnectivity requires DOD to take an active role in securing its networks. All U.S. military organizations rely on a complex networked infrastructure known as the Department of Defense Information Network (DODIN) to carry out their missions. The responsibility to protect this essential resource 24/7 falls to Joint Force Headquarters–Department of Defense Information Network (JFHQ-DODIN).

Electronic Warfare

1. **Russia winning the electronic war in Ukraine (Asia Times, 28 DEC, Gabriel Honrada)**

   Russia may already be gaining the upper hand over the electronic war in Ukraine, knocking out the latter's drones and potentially blinding its artillery.

   In an article this month in Forbes, David Axe cites a November report by the Royal United Services Institute (RUSI) that Russian electronic warfare (EW) capabilities have knocked out the majority of Ukraine's drones, with the average lifespan of a small quadcopter drone reduced to three flights, and that of fixed-wing models to six.

Information Advantage

1. **Get The 411 On Misinformation, Disinformation And Malinformation (Forbes, 13 JAN, Perry Carpenter)**

   People are exposed to misinformation and disinformation continuously. Whether it's extremist groups pedaling conspiracy and violence everywhere from Michigan to Germany, untold millions of people consume and spread disinformation and misinformation every day online. Even the WHO flagged the word "infodemic."

2. **Japan taps AI to defend against fake news in latest frontier of war (Nikkei Asia, 09 JAN, Hiroshi Asahina)**

   Japan plans to start using artificial intelligence to analyze foreign disinformation campaigns, bolstering its response to the spread of fake news across social media.

   Disinformation campaigns are part of what is called cognitive warfare -- which involves manipulating public opinion and sowing dissent through social media and other channels. Given its potential reach, it is increasingly considered a sixth domain of conflict after land, sea, air, space and the cyber realm.

3. **Ukraine Situation Report: Troop Loss Catastrophe In Donetsk Outrages Russia's Military Bloggers (The Drive, 02 JAN, Howard Altman)**

   Russia's influential military bloggers, who operate somewhat outside Moscow's tight restrictions on coverage of its 'special military operation,' are furious and heaping blame on Russian commanders after scores of troops were killed and even more were wounded in a massive Ukrainian New Year's Day attack on a converted school building in the occupied town of Makiivka.

Signal

1. **Army defines communications needs for 2030 (Army News Service, 11 Jan, SFC Michael Reinsch)**

   WASHINGTON — In war stories across a multitude of mediums, there is often a moment where a Soldier shouts into a radio to some unseen entity on the receiving end of the line. Whether it is giving a direct command or delivering information, this format of communication has been in rotation within the Army since the 1940s with the “manpack” radio, which was a relatively heavy radio that could be carried by a Soldier in a ruck.

   Since then, there have been many updates to the way the Army communicates by adding security measures and changing the platform to meet mission requirements.

2. **China developing own version of JADC2 to counter US (C4ISRNet, 5 JAN, Colin Demarest)**

   China is pursuing a new military construct known as Multi-Domain Precision Warfare to align its forces from cyber to space, an effort U.S. officials say is fueled by a need to counter the Pentagon’s Joint All-Domain Command and Control initiative.

Items of Interest

1. Russia-Ukraine Situation Report, (U.S. Army Asian Studies Detachment)

These reports are a compilation of articles from Russia, Ukraine, and other nations regarding the current tensions between Russia and Ukraine. Topics covered in this report include the following:

- Foreign Observations and Reactions
- Social Media Highlights
- Russian Eastern Military District Movements
- Other Topics

Russia-Ukraine Situation Report, 13 January 2023
Russia-Ukraine Situation Report, 12 January 2023
Russia-Ukraine Situation Report, 11 January 2023
Russia-Ukraine Situation Report, 10 January 2023
Russia-Ukraine Situation Report, 09 January 2023
Russia-Ukraine Situation Report, 05 January 2023
Russia-Ukraine Situation Report, 04 January 2023

2. The Ukraine War Is Still Relatively Low-Tech — for Now (Bloomberg, 12 JAN, Jamey Keaten)

The head of NATO expressed worry that the fighting in Ukraine could spin out of control and become a war between Russia and NATO, according to an interview released Friday.

“If things go wrong, they can go horribly wrong,” NATO Secretary-General Jens Stoltenberg said in remarks to Norwegian broadcaster NRK.

“It is a terrible war in Ukraine. It is also a war that can become a full-fledged war that spreads into a major war between NATO and Russia,” he said. “We are working on that every day to avoid that.”

3. U.S. involvement in Ukraine war deepens, with troops to train in Oklahoma (The Washington Post, 10 JAN, Dan Lamothe)

The Pentagon is planning to bring Ukrainian troops to the United States for training on the Patriot missile defense system, U.S. officials said Tuesday, signaling the Biden administration’s latest test of Russian President Vladimir Putin’s threshold for Western intervention in the conflict.

The training will occur at Fort Sill, an expansive facility covering roughly 145 square miles southwest of Oklahoma City, and could begin as soon as next week. The base is home to the U.S. military’s basic Patriot missile defense training program and another curriculum designed to teach American personnel field artillery maneuvers.

4. **South Korea Now Openly Discussing Arming Itself With Nuclear Weapons, (The Drive, 12 JAN, Thomas Newdick)**

South Korea's president has said that his country might build nuclear weapons in response to the continuing buildup of similar weapons in North Korea. This is the most explicit announcement so far from Seoul that it's actively considering nuclear weapons, although the disclosure is also very likely calculated to pressure the United States into giving Seoul a role in nuclear war planning on the peninsula, and perhaps also to redeploy U.S. tactical nuclear weapons to South Korea, the last of these having being withdrawn in 1991.