U.S. ARMY

Cyber Center of Excellence

Unclassified Threat Read Book

16 - 31 December 2023

Prepared by: Threat Management Office CCoE
Fort Gordon, GA 30905
POC: Jeffrey Hardimon & Kevin Bird
706-849-9259

Table of Contents

Israel-Hamas Conflict

1. The Drive Israel-Gaza Update
2. Institute for The Study of War Iran Update
3. Hamas Set To Pose Far-Bigger Threat Than The Islamic State; Israel Fighting A 'Monster' In Gaza: OPED - 28 DEC
4. THE ORDER OF BATTLE OF HAMAS' IZZ AL DIN AL QASSEM BRIGADES - 22 DEC
5. How Iraq is managing the Israel-Gaza crisis - 21 DEC

Russia-Ukraine Conflict

1. Russia-Ukraine Situation Report
2. Institute for The Study of War Russian Offensive Campaign Assessment
3. Russia Launches Biggest Long-Range Attack Since Start Of War - 29 DEC
4. Greatly Decreased Participation of Russian Army in 2023 Victory Day Parade Caused by Losses in Ukraine: Eastern Military District Less Impacted – 22 DEC
5. THE HIGH PRICE OF LOSING UKRAINE: PART 2 — THE MILITARY THREAT AND BEYOND - 22 DEC
6. Putin Ratchets Up Military Pressure on Ukraine as He Expects Western Support for Kyiv to Dwindle - 20 DEC

Cyber

1. **10 Most Notable Cyber Attacks of 2023 (Cyber Security News, 29 DEC, Cyber Writes Team)**

   In recent times, due to rapid advancements in technology, increased connectivity, and sophisticated tactics that threat actors use, cyber attacks are evolving at a rapid pace.

   The rise of AI (Artificial Intelligence) and ML (Machine Learning) technologies enables threat actors to:-

   - Automate their methods
   - Enhance their methods

   These seamless revolutions make it harder for security analysts and solutions to detect and mitigate evolving threats.

   Besides this, the expanding attack surface, driven by the expansion of the following things, provides more entry points for exploitation to the threat actors:-

   - IoT devices
   - Cloud services

   In 2023, many hacking events were reported, but today, we will enlist the top 10 hacks of 2023.

2. **iPhone users on TikTok are freaking out as the app is requesting sensitive personal data (Phone Arena, 28 DEC, Alan Friedman)**

   There is something that is making TikTok users with an iPhone a bit nervous. According to Reddit, the short-form video app is asking users for their iPhone passcode before allowing them to continue to use the app. We recently showed you an interview with a cybercriminal who ripped off people for an amount estimated to be anywhere between $300,000 and $2 million. His MO was to watch iPhone users punch in their passcode, steal the iPhone; and take control of that device inside of 10 minutes.

3. **Financially motivated threat actors misusing App Installer (Microsoft, 28 DEC, Microsoft Threat Intelligence)**

   Since mid-November 2023, Microsoft Threat Intelligence has observed threat actors, including financially motivated actors like Storm-0569, Storm-1113, Sangria Tempest, and Storm-1674, utilizing the ms-appinstaller URI scheme (App Installer) to distribute malware. In addition to ensuring that customers are protected from observed attacker activity, Microsoft investigated the use of App Installer in these attacks. In response to this activity, Microsoft has disabled the ms-appinstaller protocol handler by default.

4. **Addressing the Growing Threat of Supply Chain Cyberattacks (Hacker Noon, 21 DEC, Patracia de Hemricourt)**

   Supply chain cyber-attacks are on the rise. These attacks infiltrate a company's network through a trusted third-party supplier that has been breached. With more businesses outsourcing services and adopting cloud solutions, the potential entry points for attackers have expanded.

   Recent examples like the famous SolarWinds Orion supply chain attack demonstrate how compromising one vendor can have massive downstream impacts. By penetrating SolarWinds' software development environment, attackers inserted malicious code into Orion updates which granted access to thousands of public and private sector

organizations upon installation.

5. **86% of cyberattacks are delivered over encrypted channels (Help Net Security, 21 DEC)**

Threats over HTTPS grew by 24% from 2022, underscoring the sophisticated nature of cybercriminal tactics that target encrypted channels, according to Zscaler

For the second year in a row, manufacturing was the industry most commonly targeted, with education and government organizations seeing the highest year-over-year increase in attacks. Additionally, malware, which includes malicious web content and malware payloads, continued to dominate over other types of encrypted attacks, with ad spyware sites and cross-site scripting accounting for 78% of all blocked attacks.

In total, 86% of all cyber threats, including malware, ransomware, and phishing attacks, are delivered over encrypted channels.

6. **Top 10 cyber crime stories of 2023 (Computer Weekly, 21 DEC, Alex Scroxton)**

Ransomware gangs dominated the cyber criminal underworld in 2023, a year that will prove notable for significant evolutionary trends in their tactics

Back to Table of Contents

When it comes to cyber crime, it's easy to assume that there is nothing new under the sun. After all, the whole point of cyber crime – to a cyber criminal – is to get someone else's money in their pockets as quickly as possible. What could be more effective a tool than ransomware?

However, even perfect systems can be improved around the margins, tried-and-tested methods can be tweaked, and incremental adjustments made. So it was in 2023, which will be remembered as the year in which the already commodified ransomware ecosystem started to do away with actual ransomware, in favour of mass targeting of victims and straight-up data theft and extortion.

7. **This Means Cyber War: Chinese Hackers Target Critical U.S. Infrastructure (The Federalist, 18 DEC, Helen Raleigh)**

If the Chinese Communist Party invades Taiwan, Chinese military-affiliated hackers will likely disrupt critical infrastructure in the U.S.

2023 will go down in history as the year that China's state-sponsored hackers advanced their ability to wage cyber warfare against the U.S.

Chinese hackers used to focus on stealing America's commercial secrets and personnel information (see examples here and here). But this year, Chinese hackers have expanded their reach by collecting intelligence on U.S. government agencies and breaching systems of infrastructures with strategic value.

Electronic Warfare

1. **Air Force publishes new doctrine on electromagnetic spectrum operations (Defense Scoop, 27 DEC, Mark Pomerleau)**

   The U.S. Air Force released new doctrine for electromagnetic spectrum operations, reflecting a change in the operating environment.

   The document, published Dec. 14, outlines concepts, terminology, roles and responsibilities, authorities, operations and the importance of the spectrum to joint ops.

   "The joint force requires an overmatching, offensive approach to electromagnetic spectrum operations (EMSO) to enhance competitive advantage and create multiple dilemmas for adversaries in all domains. Airmen should develop EMS awareness, engagement, and maneuver capabilities that span and connect all domains and enable successful friendly operations," the foreword states. "Dominant EMS expertise and capabilities can render adversary sensors, situational awareness, command and control, networks, and decision processes ineffective, preventing adversaries from attaining their objectives."

2. **More And More Russian Vehicles Have Drone-Jammers. Ukrainian Drones Blow Them Up Anyway. (Forbes, 22 DEC, David Axe)**

   Russian industry developed the RP-377 jammer to interfere with enemy soldiers' radio communications. As it happens, the jammer also works against radio-controlled first-person-view drones.

   But only at very short range. And that helps to explain why Ukrainian drone-pilots have been blowing up Russian vehicles sporting RP-377s. A skilled operator can aim their drone at a vehicle, and count on the drone's momentum to propel it to a successful strike even as its radio control link drops out in the final few seconds of its flight.

   It seems Ukrainian operators have had to figure this out on their own, however. According to Ukrainian drone expert Serhii Beskrestnov, the Ukrainian defense ministry hasn't helped.

Back to Table of Contents

3. **Czech Republic receives new electronic surveillance system (Janes, 15 DEC, Olivia Savage)**

   The Army of the Czech Republic (ACR) has received the first of two new deployable passive electronic surveillance systems following an official handover ceremony to the 532nd Electronic Warfare Battalion on 13 December.

   The system, known as the Deployable Passive Electronic Support Measures Tracker (DPET), is replacing the in-service Vera-S/M, although it will remain in the armament of the army and be used for training and use by Active Reserve units, according to an announcement by the Armed Forces of the Czech Republic.

   The DPET will be in service over the next 10–15 years following delivery of the second and final system in 2024

   .

Information Advantage

1. China's Influence Operations and Cognitive Warfare in Taiwan, 27 December 2023 (U.S. Army Asian Studies Detachment, 28 DEC)

This report, based primarily on Taiwanese sources, details China's efforts to influence and subvert Taiwan, the U.S., Japan, and other major countries in the region.

Contents

2. BRI - Belt and Road Initiative - Highlights, 22 December 2023 (U.S. Army Asian Studies Detachment, 22 DEC)

The Belt and Road Initiative (BRI) is an expansive economic and infrastructure program initiated by the People's Republic of China aimed at increasing its influence throughout the world. Targeted primarily at poorer nations, or nations the PRC has a strategic interest in, it aims to increase the infrastructure usable by the PRC as well as making those nations economically dependent upon the PRC.

The following is a compilation of reports covering projects the PRC will initiate or have already started, as well as covering the evaluation or criticism of BRI in local countries and diplomatic efforts by China to promote BRI.

ASD is publishing BRI-related reports on PiX, the Protected Internet eXchange Portal, which can be viewed at the following URL: hxxps://pixtoday.net/article/article/220079.

Contents of this report

4) Media Cooperation Efforts Under BRI / Media Efforts to Promote BRI

3. Foreign Reflections on U.S. Exercises and Operations, 22 December 2023 (U.S. Army Asian Studies Detachment, 22 DEC)

This report is an examination of foreign reactions in the Asia-Pacific region to U.S. bilateral and multilateral exercises, and other United States Department of Defense activities such as weapons transfers and sales, military exchanges, and military operations. This report iteration covers relevant reporting from 11-21 December and gathers media coverage from China, North Korea, and Japan.

4. Government watchdog prepares to assess Pentagon's revamped AI strategy (Defense Scoop, 21 DEC, Brandi Vincient)

In early 2024, government oversight officials will meet with multiple Defense Department teams and formally review the agency's new Data, Analytics, and Artificial Intelligence Adoption Strategy — to ultimately assess whether it fulfills guidance they provided in a March 2022 report.

A watchdog study published last year urged DOD to improve its frameworks, inventory processes and official approaches for incorporating the powerful, still-maturing technology.

5. Deepfakes Aren't the Disinformation Threat They're Made Out to Be (RAND, 19 DEC, Peter Carlyon)

The chief of Britain's domestic intelligence agency MI5 warns of danger on the horizon. Deepfakes, Ken McCallum said at a conference in California, are "a threat to democracy" with the potential to "cause all kinds of confusion and dissension and chaos in our societies."

It's a warning often repeated—yet one that always seems just around the corner.

Deepfakes—imitative audio-visual content produced via deep learning techniques—have been on the radar of media watch organizations for years, and there's no doubt they can be convincing. In 2017, a researcher from the University of Washington shared an artificial video of a foul-mouthed Barack Obama, prompting tech experts to warn of an impending crisis if generative AI was left unchecked.

6. Enhancing trust and protecting privacy in the AI era (Microsoft, 19 DEC, Julie Brill)

At Microsoft we want to empower our customers to harness the full potential of new technologies like artificial intelligence, while meeting their privacy needs and expectations. Today we're sharing key aspects of how our approach to protecting privacy in AI – including our focus on security, transparency, user control, and continued compliance with data protection requirements – are core components of our new generative AI products like Microsoft Copilot.

We create our products with security and privacy incorporated through all phases of design and implementation. We provide transparency to enable people and organizations to understand the capabilities and limitations of our AI systems, and the sources of information that generate the responses they receive, by providing information in real-time as users engage with our AI products. We provide tools and clear choices so people can control their data, including through tools to access, manage, and delete personal data and stored conversation history.

7. A clunky Chinese disinformation effort has spread to all corners of

the internet (The Guam Daily Post, 18 DEC, Margi Murphy)

When a Twitter account for Utah business coach Spencer Taggart began posting about hot-button political issues in 2020, it garnered widespread attention. Tweets about an endemic cultural divide in the U.S. and support for Black Lives Matter were shared by two Chinese embassy officials.

But Taggart didn't write the tweets and hasn't been on the social media platform, now called X, in five years. Rather, his identity had been hijacked by a massive pro-China propaganda network, according to the social media analysis firm Graphika.

8. The rise of AI fake news is creating a 'misinformation superspreader' (The Washington Post, 17 DEC, Pranshu Verma)

Artificial intelligence is automating the creation of fake news, spurring an explosion of web content mimicking factual articles that instead disseminates false information about elections, wars and natural disasters.

Since May, websites hosting AI-created false articles have increased by more than 1,000 percent, ballooning from 49 sites to more than 600, according to NewsGuard, an organization that tracks misinformation.

Historically, propaganda operations have relied on armies of low-paid workers or highly coordinated intelligence organizations to build sites that appear to be legitimate. But AI is making it easy for nearly anyone — whether they are part of a spy agency or just a teenager in their basement — to create these outlets, producing content that is at times hard to differentiate from real news.

Back to Table of Contents

9. BRI - Belt and Road Initiative - Highlights, 13 December 2023 (U.S. Army Asian Studies Detachment, 18 DEC)

The Belt and Road Initiative (BRI) is an expansive economic and infrastructure program initiated by the People's Republic of China aimed at increasing its influence throughout the world. Targeted primarily at poorer nations, or nations the PRC has a strategic interest in, it aims to increase the infrastructure usable by the PRC as well as making those nations economically dependent upon the PRC.

The following is a compilation of reports covering projects the PRC will initiate or have already started, as well as covering the evaluation or criticism of BRI in local countries and diplomatic efforts by China to promote BRI.

ASD is publishing BRI-related reports on PiX, the Protected Internet eXchange Portal, which can be viewed at the following URL: hxxps://pixtoday.net/article/article/220079.

Contents of this report

1) Official Chinese Government Announcements on BRI
2) Progress of BRI Projects outside China
3) Reviews and Critiques by Countries on BRI
4) Diplomatic / Media Efforts to Promote BRI.

Signal

1. **Air Force taps Intelsat for commercial space internet project (Defense Scoop, 29 DEC, Jon Harper)**

   The Air Force Research Lab has added Intelsat to its list of vendors for the Defense Experimentation Using Commercial Space Internet (DEUCSI) program.

   As part of the initiative, AFRL plans to conduct a set of demonstrations that will aim to provide military aircraft with ubiquitous connectivity using commercial spacecraft and networks.

   The Pentagon announced the $9 million deal with Intelsat on Wednesday.

   "This contract provides for efforts to develop and experimentally test satellite communications (SATCOM) systems capable of operating with multiple commercial space internet constellations operating in low, medium, and geostationary earth orbits offering a new low size, weight, power, and cost (SWaP-C) terminal that easily integrates onto aircraft platforms to provide resilient, high throughput, globally available, and highly reliable SATCOM," per the announcement.

Back to Table of Contents

2. **Russia Flaunts 'Magic Radio' To Shield Its FVP Drones From Jamming, Thwart Electronic Warfare Attacks (The EurAsian Times, 24 DEC, Ritu Sharma)**

   The Russia-Ukraine war has proved to be a breeding ground for electronic warfare. Russia claims to have developed a 'magic radio' for FPV (First Person View) drones that will make them highly resistant to jamming in the latest technological development for drones.

   The innovation is another testament to how off-the-shelf consumer technology is used in a military environment. Both Russia and Ukraine are augmenting their FPVs manufacturing capabilities.

   Sudoplatov, a Russian group, asserts that they manufacture a thousand of them daily. Dominating the electronic spectrum to jam the adversary's drones and making drones foolproof against disruption has, thus, become crucial on the battlefield. A dominance in electronic warfare will allow one to subvert the enemy while remaining unharmed.

3. **Ukraine Gets 5,000 Starlink Terminals From Poland Six Months After Elon Musk Opposed Its 'Battlefield' Use (The EurAsian Times, 22 DEC, Parth Satam)**

   Ukraine has reportedly acquired 5,000 Starlink terminals from Poland, which Kyiv had previously used to guide its UAVs and battlefield military communications. The development comes three months after SpaceX founder Elon Musk denied Starlink's coverage over Crimea for Ukraine to attack Russia's Black Sea Fleet.

   Ukraine's unmanned naval kamikaze boat had targeted Russia's Black Sea Fleet (BSF) anchored at Sevastopol, successfully hitting warships and the headquarters earlier this year.

   On previous occasions, Musk had expressed reservations over using the Starlink satellite internet service for military purposes. He had warned about escalation that could lead to a larger war.

Items of Interest

1. **After U.S. Navy Helicopters Sink Houthi Boats Are Strikes Next? (The Drive/The Warzone, 31 DEC, Tyler Rogoway)**

   Navy MH-60 Sea Hawks sink Houthi boats after being fired upon as anti-ship ballistic missiles fly across the Red Sea.

   Things are really heating up in the southern end of the Red Sea. Houthi attacks on shipping moving through the chokepoint not only continue, but appear to be getting more complex. Now U.S. Central Command has said Navy helicopters were fired upon by Houthi raiding craft while responding to a distress call from a cargo ship. The helicopters fired back, sinking the boats. This comes as a report claims the U.S. and the U.K. are planning to strike back against Houthi forces.

   The statement from CENTCOM about the latest incident reads as follows:

   "Iranian-backed Houthi small boats attack merchant vessel and U.S. Navy helicopters in Southern Red Sea

   On Dec. 31 at 6:30am (Sanaa time) the container ship MAERSK HANGZHOU issued a second distress call in less than 24 hours reporting being under attack by four Iranian-backed Houthi small boats. The small boats, originating from Houthi-controlled areas in Yemen, fired crew served and small arms weapons at the MAERSK HANGZHOU, getting to within 20 meters of the vessel, and attempted to board the vessel. A contract embarked security team on the MAERSK HANZGHOU returned fire. U.S. helicopters from the USS EISENHOWER (CVN 69) and GRAVELY (DDG 107) responded to the distress call and in the process of issuing verbal calls to the small boats, the small boats fired upon the U.S. helicopters with crew served weapons and small arms. The U.S. Navy helicopters returned fire in self-defense, sinking three of the four small boats, and killing the crews. The fourth boat fled the area. There was no damage to U.S. personnel or equipment."

   UKMTO has put out a warning regarding this latest escalation. Reports state that at least 10 Houthi fighters were killed in the skirmish.

2. **Red Sea Attacks Continue, India Enhances Naval Posture (Updated) (The Drive/The Warzone, 26 DEC, Thomas Newdick)**

   With anti-ship strikes now taking place farther south in the Indian Ocean, India is deploying destroyers and maritime patrol aircraft.

   With the recent spate of attacks on commercial shipping now extending far out from the Red Sea and Gulf of Aden, the Indian Navy has announced the deployment of warships and maritime patrol aircraft to “maintain a deterrent presence” out into the Arabian Sea.

   The move comes after a suspected drone attack on the tanker M/V Chem Pluto about 120 miles off the Indian coast over the weekend, which

3. **Cracks Form In New Naval Coalition, Drone Strikes Spread To Indian Ocean (The Drive/The Warzone, 23 DEC, Tyler Rogoway)**

   Some of the United States’ closest allies are not agreeing to put their ships under U.S. Navy command for Operation Prosperity Guardian.

   Operation Prosperity Guardian, the American-led coalition to defend shipping through the Red Sea, the Bab el-Mandeb Strait, and the Gulf of Aden from Houthi attacks is showing major cracks just as it is forming. At the same time, the latest rash of drone strikes on commercial vessels appears to have spread far from Yemen's shores, to waters off India.

A total of twenty countries have agreed to take part in the multi-national naval security coalition, according to the Pentagon earlier this week, and some of those participants don't want to be named. One of the biggest issues is that of those 20, only a fraction will supply actual ships or other major assets to help the cause. In fact, many are just sending a handful of personnel. This is especially problematic now that Spain, Italy, and France have rejected the U.S. demand that their vessels fall under U.S. Navy command while deployed as part of the security operation.

4. Red Sea Task Force Grows, How It Actually Will Work Remains Unclear (The Drive/The Warzone, 21 DEC, Howard Altman)

As the Houthis hurled threats at the U.S. Navy, more than 20 nations are set to participate in Operation Prosperity Guardian in some manner.

Operation Prosperity Guardian (OPG), the newly formed international coalition to protect commercial shipping from Houthi attacks, will be akin to a highway patrol on the Red Sea, the Pentagon's top spokesman said Thursday. The coalition was formed in response to scores of attacks on vessels that began in the wake of the Israel-Hamas war.

"It's very important to understand that Houthis aren't attacking just one country, they're really attacking the international community," Air Force Maj. Gen. Pat Ryder told reporters, including from The War Zone. "They are attacking the economic well-being and prosperity of nations around the world. So in effect, they've really become bandits along the international highway that is the Red Sea. The forces assigned to Operation Prosperity Guardian will serve as a highway patrol of sorts, patrolling the Red Sea and the Gulf of Aden to respond to and assist as necessary commercial vessels that are transiting this vital international waterway."

5. Inside The Private Security Forces Protecting Red Sea Shipping (The Drive/The Warzone, 21 DEC, Howard Altman)

How armed contractors operate aboard ships and the ways they've been adapted to the eruption in hostilities around the Bab el-Mandeb strait.

Nearly every day, private armed security teams (PASTs) stationed on a floating armory somewhere in the Indian Ocean will get a message from supervisors at Ambrey, a U.K.-based firm specializing in maritime risk management. They are to grab their L1A1 SLR or Steyr Scout rifles and head out to a commercial ship sailing to the narrow and increasingly dangerous Bab al-Mandab Strait.

Once on board, the PAST will provide armed security, overwatch and help the crews take all the safety precautions possible for a trip through waters where U.S. Defense Secretary Lloyd Austin said Iranian-backed Houthi rebels have conducted over 100 drone and ballistic missile attacks, targeting 10 merchant vessels in the past month. This is in addition to boarding attempts and even seizing ships outright. These activities are ongoing in a region that's already a piracy epicenter.

6. Houthi attacks rocking Red Sea trade routes likely won't end anytime soon. Here's what could happen next (CNBC, 21 DEC, Natasha Turak)

KEY POINTS

- U.S. Central Command over the weekend said it shot down "14 unmanned aerial systems launched as a drone wave from Houthi-controlled areas of Yemen" in the Red Sea.
- Many tankers and cargo ships that would normally transit via the Suez Canal to the Indian Ocean are instead being rerouted around the continent of Africa.

- Yemen's Houthis have made clear their intention of targeting Israeli ships and any ships headed to or from Israel, in retaliation for the country's war in Gaza.

7. Why Hasn't The U.S. Struck Back After Red Sea Anti-Ship Attacks? (The Drive/The Warzone, 17 DEC, Tyler Rogoway)

Many are calling for strikes on Houthi forces after multiple anti-ship attacks off Yemen's coast, but is that really the best option?

My inbox has been flooded with people wanting to know why the United States has not retaliated against Houthi forces in Yemen after repeated anti-ship attacks near the Bab el-Mandeb strait — the critical funnel that connects the Red Sea with the Gulf Of Aden. It's an entirely fair question and the answer is not as simple as some would make it seem. So let's dig into it.

One prevailing viewpoint is that the Houthis will 'only understand force' and that the United States needs to hit them back. Some declare that this should have happened after the first weapons were launched at ships, but especially now.

.

Back to Table of Contents

Israel-Hamas Conflict

1. The Drive/The Warzone Israel-Gaza Update

Israel-Gaza Situation Report: U.S. Military Leaders Push For Scaled-Back Campaign – 19 DEC

2. Institute for The Study of War Iran Update:

The Iran Update provides insights into Iranian and Iranian-sponsored activities abroad that undermine regional stability and threaten US forces and interests. It also covers events and trends that affect the stability and decision-making of the Iranian regime.

Iran Update, December 31, 2023
Iran Update, December 30, 2023
Iran Update, December 29, 2023
Iran Update, December 28, 2023
Iran Update, December 27, 2023
Iran Update, December 26, 2023
Iran Update, December 24, 2023
Iran Update, December 23, 2023
Iran Update, December 22, 2023
Iran Update, December 21, 2023
Iran Update, December 20, 2023
Iran Update, December 19, 2023
Iran Update, December 18, 2023
Iran Update, December 17, 2023
Iran Update, December 16, 2023

Back to Table of Contents

3. Hamas Set To Pose Far-Bigger Threat Than The Islamic State; Israel Fighting A 'Monster' In Gaza: OPED (The EurAsian Times, 28 DEC, Salah Uddin Shoaib Choudhury)

Ever since assuming office, US President Joe Biden has been consistently misleading the world with lies and fabricated stories, thus further deepening the risks posed by Islamist militancy outfits, including Islamic State (ISIS), Al Qaeda, Hezbollah, Hamas, Houthis, and others. Abruptly ending the 'War on Terror' and withdrawing US troops from Afghanistan was a disastrous blunder.

Meanwhile, the Palestinian terrorist outfit Hamas has succeeded in expanding its network within Western countries, where the number of its fighters is already much more significant than that of Islamic State (ISIS) and Al Qaeda.

This was proved when seven terrorists, including four Hamas members, were arrested in Denmark, Germany, and the Netherlands on suspicion of planning attacks on Jewish institutions in Europe. The arrests were made as Israel pressed on with its operation to destroy Hamas in the Gaza Strip following the October 7 Hamas pogrom in Israel.

4. THE ORDER OF BATTLE OF HAMAS' IZZ AL DIN AL QASSEM BRIGADES (ISW, 22 DEC, Brian Carter)

The al Qassem Brigades are the military component of Hamas and the means by which Hamas seeks to destroy the Israeli state and form an Islamic state in Palestine. Hamas

is a highly organized group that views terrorism and military action as the only method through which it can destroy the Israeli state. The al Qassem Brigades are commanded by Mohammad Deif and are subordinated to the overall Hamas political leadership responsible to Ismail Haniyeh. They coordinate closely with the Hamas political leader in the Gaza Strip, Yahya Sinwar. Hamas defines itself as a "Palestinian national liberation and resistance movement" intent on establishing an Islamic Palestinian state that stretches "from the River Jordan...to the Mediterranean and from Ras al Naqurah [Israel's northern border with Lebanon]...to Umm al Rashrash [Eilat—Israel's southernmost city]"—in other words, all the territory of Israel. It is also a member of Iran's "Axis of Resistance," the regional coalition of states and groups that Tehran has built as part of its effort to destroy Israel and expel the United States from the Middle East. Hamas states that "armed resistance" is a "strategic choice" to protect the Palestinian people and rejects "any attempt to undermine [Hamas'] resistance." Hamas is fighting alongside other Palestinian resistance groups such as Palestinian Islamic Jihad and the Popular Front for the Liberation of Palestine, with which it engages in operational and tactical coordination.

5. How Iraq is managing the Israel-Gaza crisis (Brookings, 21 DEC, Marsin Alshamary & Kevin Huggard)

Editor's note: This piece is part of the Center for Middle East Policy's Israel-Gaza interviews series, in which leading experts unpack the conflict via in-depth Q&As.

Russia-Ukraine Conflict

1. The Drive/The Warzone Ukraine Situation Report:

Ukraine Situation Report: Zelensky Appears Near Front In Avdiivka – 29 DEC
Ukraine Situation Report: Are Air Losses Pushing A Shift In Russian Tactics? – 26 DEC
Ukraine Situation Report: Kyiv Wants A Million FPV Drones In 2024 – 20 DEC
Ukraine Situation Report: U.S. Funding Almost "Exhausted" – 18 DEC
Ukraine Situation Report: Troops Question Dnipro River Assault – 16 DEC

2. Institute for The Study of War

Russian Offensive Campaign Assessment, December 31, 2023
Russian Offensive Campaign Assessment, December 30, 2023
Russian Offensive Campaign Assessment, December 29, 2023
Russian Offensive Campaign Assessment, December 28, 2023
Russian Offensive Campaign Assessment, December 27, 2023
Russian Offensive Campaign Assessment, December 26, 2023
Russian Offensive Campaign Assessment, December 24, 2023
Russian Offensive Campaign Assessment, December 23, 2023
Russian Offensive Campaign Assessment, December 22, 2023
Russian Offensive Campaign Assessment, December 21, 2023
Russian Offensive Campaign Assessment, December 20, 2023
Russian Offensive Campaign Assessment, December 19, 2023
Russian Offensive Campaign Assessment, December 18, 2023
Russian Offensive Campaign Assessment, December 17, 2023
Russian Offensive Campaign Assessment, December 16, 2023

Back to Table of Contents

3. Russia Launches Biggest Long-Range Attack Since Start Of War (The Drive/The Warzone, 29 DEC, Thomas Newdick)

More than 100 missiles and dozens of one-way attack drones rained down on at least six Ukrainian cities overnight.

Russia launched an apparently unprecedented wave of missile and drone strikes against Ukraine overnight. If the claims of Ukrainian authorities are correct, and 122 missiles were indeed launched, together with 36 one-way attack drones, this would be the biggest air raid of its kind since the start of the Kremlin's full-scale invasion in February 2022.

Based on Ukrainian Air Force figures, previously the biggest assault was in November 2022 and involved 96 missiles launched against Ukraine. The heaviest attack this year was on March 9, involving 81 missiles.

4. Greatly Decreased Participation of Russian Army in 2023 Victory Day Parade Caused by Losses in Ukraine: Eastern Military District Less Impacted (U.S. Army Asian Studies Detachment, 22 DEC)

Russia held its 78th Victory Day parade on 9 May 2023, the anniversary of Nazi Germany's surrender to allied forces. Russia has traditionally held these parades in 28 major cities and other locations, with the largest parade held in Moscow's Red Square. The scale and scope of the 2023 Victory Day Parades are significantly less than the 76th parades2021 parades, the last before Russia launched hostilities in Ukraine in February

2022. This is a likely indication of how the war in Ukraine has depleted Russian ground forces. OSINT for this report was gathered with an ASD partner, the Japan Ground Self Defense Force Basic Intelligence Unit., then vetted.

5. THE HIGH PRICE OF LOSING UKRAINE: PART 2 — THE MILITARY THREAT AND BEYOND (ISW, 22 DEC, Nataliya Bugayova)

Allowing Russia to win its war in Ukraine would be a self-imposed strategic defeat for the United States. The United States would face the risk of a larger and costlier war in Europe. The United States would face the worst threat from Russia since the collapse of the Soviet Union, as a victorious Russia would likely emerge reconstituted and more determined to undermine the United States — and confident that it can. A Russian victory would diminish America's deterrence around the world, emboldening others with an explicit or latent intent to harm the United States. A Russian victory would create an ugly world in which the atrocities associated with Russia's way of war and way of ruling the populations under its control are normalized.

Most dangerous of all, however, US adversaries would learn that they can break America's will to act in support of their strategic interests. The ground truths of this war have not changed: Russia still explicitly intends to erase Ukraine as a concept, people, and state; Ukraine's will to fight remains strong; Russia has made no operationally significant advances this year; and Ukraine's will combined with the West's collective capability (which dwarfs Russia's) can defeat Russia on the battlefield.[1] US interests still include preventing future Russian attacks on Ukraine and helping Ukraine liberate its people and territory. Supporting Ukraine is still the best path for the United States to avoid higher costs, larger escalation risks, and a greater Russian threat. What's changing is Americans' perceptions of their interests, not the interests themselves. That American perceptions are changing is not an accident. It is, in fact, precisely the effect the Kremlin has been seeking to achieve. The Kremlin's principal effort is destroying America's will by altering Americans' understanding of their interests, and this effort appears to be working. If Russia wins in Ukraine because of the collapse of Western aid, it will be because Russia has managed to shape Americans' understanding of reality such that the United States willingly chooses to act against its interests and values without realizing that it is doing so. Russia will have manipulated America into abandoning its own interests in a fight it could and should have won. That's a dangerous lesson for China, Iran, and other US adversaries to learn. America's security now and in the future, in Asia and the Middle East as well as in Europe, depends on remaining solidly connected with our strategic interests and values and demonstrating that we will not fall prey to efforts to manipulate our perceptions of those interests.

6. Putin Ratchets Up Military Pressure on Ukraine as He Expects Western Support for Kyiv to Dwindle (AP News, 20 DEC)

After blunting Ukraine's counteroffensive from the summer, Russia is building up its resources for a new stage of the war over the winter, which could involve trying to extend its gains in the east and deal significant blows to the country's vital infrastructure.

Russian President Vladimir Putin seems to be hoping that relentless military pressure, combined with changing Western political dynamics and a global focus on the Israeli-Hamas war, will drain support for Ukraine in the nearly 2-year-old war and force Kyiv to yield to Moscow's demands.