



**Risk Mitigation Consulting Inc.**

*Intelligence and Analysis Division*

# OPEN SOURCE UPDATE

February 2020

## **INTENT**

This open source periodical is designed to provide an overview of relevant, publicly available information on threat and hazard events and analysis of potential impacts to the interests of the United States, both at home and abroad. This product is not intended to be a comprehensive overview of all threat and hazard news and inclusion in this product does not constitute a confirmation of credibility nor precedence by RMC.



<b>Threats</b>	Page
<b>U.S. Marine Corps Limits Base Access by Foreign Nationals</b> <i>Insider Threat</i>	2
<b>Raytheon Engineer Pleads Guilty to Federal Arms Export Charges</b> <i>Insider Threat</i>	2
<b>Chinese Military Members Charged by U.S. in Connection With 2017 Equifax Hack</b> <i>FIE</i>	3
<b>Google Removes Over 500 Malicious Chrome Browser Extensions</b> <i>Cyber</i>	4

<b>Hazards</b>	Page
<b>Record High Temperatures in Antarctica</b> <i>Meteorological Hazards</i>	6
<b>DoD Installations May Serve as Coronavirus Quarantine Sites</b> <i>Biological Hazards</i>	7
<b>Locust Outbreak in East Africa</b> <i>Biological Hazards</i>	7
<b>U.S. Nuclear Waste May Be Stored Unsafely</b> <i>Accidental Events</i>	8



## Threats

### **U.S. Marine Corps Limits Base Access by Foreign Nationals – *Insider Threat***

**Excerpt:** The Corps has placed new restrictions on foreign troops' access to Marine Corps installations in an attempt to improve base security in the wake of a base shooting by a foreign military student who killed three sailors and wounded eight others.

Royal Saudi Air Force Lt. Mohammed Saeed Alshamrani was a student naval flight officer on base on Dec. 6. at Naval Air Station Pensacola, Florida.

The change applies to common access cards, or CACs, with a blue stripe issued to foreign military students, liaison officers and participants in the personnel exchange program, according to a 06 February administrative message announcing the policy.

Once in effect, the blue-striped CAC cards will give the holder permission to access only the bases where they are assigned, unless they receive special permission on a case-by-case basis, the MARADMIN said. Their CAC cards previously gave access to all bases.

**Analyst Comment:** The December 2019 shooting by a visiting Saudi Royal Air Force student onboard NAS Pensacola has renewed concerns regarding vetting of visiting foreign military personnel at DoD installations. The Marine Corps has decided to establish policy restricting access to its installations by foreign military personnel to include access to the base(s) to which they are assigned. However, it is important to note that Alshamrani (the perpetrator of the NAS Pensacola shooting) was authorized to be onboard NAS Pensacola at the time of the incident. Still, restricting individuals' access to areas that are not necessary for the performance of their duties is a sound practice for security.

In the wake of the NAS Pensacola shooting, Secretary of Defense Mark Esper recently announced that foreign military students will be subject to increased vetting from DoD, to include social media monitoring as well as continuous monitoring during their time inside the U.S. A similar process is established and growing in order to continuously evaluate individuals' eligibility for security clearances.

Source: <https://www.marinecorpstimes.com/news/your-marine-corps/2020/02/11/marine-corps-to-limit-base-access-for-foreign-nationals-in-wake-of-pensacola-shooting/>

---

### **Raytheon Engineer Pleads Guilty to Federal Arms Export Charges – *Insider Threat***

**Excerpt:** A naturalized U.S. citizen from China who worked for 10 years for a Raytheon Corp. subsidiary as an electrical engineer has pleaded guilty to a federal arms exportation charge.



Wei Sun pleaded guilty in U.S. District Court in Tucson, where Raytheon Missile Systems has a large defense plant that produces missiles.

In a plea agreement with prosecutors, Sun acknowledged taking a Raytheon laptop to China on a 2018 personal trip and acknowledged that it contained sensitive material, including a user's guide for an air-to-air missile.

A five-count indictment charging Sun did not allege he actually shared any of the information but merely moving sensitive weapons files out of the country without permission violates federal law on arms exports.

**Analyst Comment:** Sun worked on highly sensitive missile programs used by the US military. Since Sun's computer contained large amounts of restricted data, Raytheon officials told him that taking it abroad would not only be a violation of company policy, but a serious violation of federal law. However, Sun still brought his laptop abroad. While he was out of the country, Sun connected to Raytheon's internal network on the laptop. He sent an email suddenly announcing he was quitting his job after 10 years in order to study and work overseas.

When Sun returned to the United States a week later, he told Raytheon security officials that he had only visited Singapore and the Philippines during his travels. But inconsistent stories about his itinerary led Sun to confess that he traveled to China with the laptop.

Many of the projects Sun was involved with could be of interest to the Chinese government. Though there is no indication that the information was intended to be sold or shared, the event highlighted an insider threat at a cleared defense contractor with potentially serious consequences.

Source: <https://www.usnews.com/news/best-states/arizona/articles/2020-02-15/former-raytheon-engineer-pleads-guilty-to-weapons-count>

---

## Chinese Military Members Charged by U.S. in Connection With 2017 Equifax Hack – *FIE*

**Excerpt:** Four members of China's military were charged with hacking into Equifax, one of the nation's largest credit reporting agencies, and stealing trade secrets and the personal data of about 145 million Americans in 2017.

The charges underscored China's quest to obtain Americans' data and its willingness to flout a 2015 agreement with the United States to refrain from hacking and cyberattacks, all in an effort to expand economic power and influence.

The indictment suggests the hack was part of a series of major data thefts organized by the People's Liberation Army and Chinese intelligence agencies. China can use caches of personal information and combine them with artificial intelligence to better target American intelligence officers and other officials, Attorney General William P. Barr said.



The information stolen from Equifax, which is based in Atlanta, could reveal whether any American officials are under financial stress and thus susceptible to bribery or blackmail.

**Analyst Comment:** The indictment of four Chinese military members for their role in the 2017 Equifax hack highlights the intelligence value of personal information. Equifax is a major credit reporting agency, which hosts personally identifiable financial information on over 800 million consumers and 88 million businesses worldwide. Over 145.5 million U.S. consumers were affected in the 2017 breach, likely to include a significant number of individuals who would be of intelligence value to Chinese interests. Individuals in fields to include defense, aerospace, security, and technology who had apparent financial difficulties could potentially be targeted by China-affiliated actors and bribed/blackmailed for information.

U.S. officials also expressed concerns that this financial data, when paired with other data sets (to include travel and health history) could be leveraged using artificial intelligence to provide China with more actionable target lists for the cultivation of intelligence assets.

Source: <https://www.zdnet.com/article/google-removes-500-malicious-chrome-extensions-from-the-web-store/>

---

## Google Removes Over 500 Malicious Chrome Browser Extensions – Cyber

**Excerpt:** Google has removed more than 500 malicious Chrome extensions from its official Web Store following a two-months long investigation conducted by security researcher Jamila Kaya and Cisco's Duo Security team.

The removed extensions operated by injecting malicious ads (malvertising) inside users' browsing sessions.

The malicious code injected by the extensions activated under certain conditions and redirected users to specific sites. In some cases, the destination would be an affiliate link on legitimate sites like Macys, Dell, or BestBuy; but in other instances, the destination link would be something malicious, such as a malware download site or a phishing page.

According to a report published and shared with ZDNet, the extensions were part of a larger malware operation that's been active for at least two years.

**Analyst Comment:** Google's Chrome web browser is one of the most prominent browsers in the world. As of October 2019, Chrome had significantly more worldwide market share than competitors such as Mozilla Firefox, Apple's Safari, and Microsoft's Edge and Internet Explorer. Chrome also has a number of browser extensions: additional pieces of software that can enhance the capabilities of the browser, such as blocking ads or adding productivity tools. However, security researchers discovered a number of browser extensions that were directing users to malicious sites that were designed to install malware or phish (attempt to steal the personal



information of) users. Fortunately, Google took action to remove the malicious browser extensions from the Chrome app store. Still, it is possible that additional malicious browser extensions are present, and users of these extensions should evaluate the source of (and permissions granted to) such extensions for authenticity, credibility and security.

*Source:* <https://www.zdnet.com/article/google-removes-500-malicious-chrome-extensions-from-the-web-store/>

---



## Hazards

### Record High Temperatures in Antarctica – *Meteorological Hazards*

**Excerpt:** The Antarctic Peninsula is recovering from a heat wave that has redefined t-shirt weather on the world's largest frozen landmass and raised alarm bells about its future. Weather stations near the northern tip of the peninsula and on neighboring islands recently logged temperatures in the mid-60s and even one near 70-degree reading. If confirmed, they will stand as new high temperature records for the continent.

A mix of meteorological factors, from warm mountain winds to larger patterns in the ocean and atmosphere, are responsible for the balmy blast. But the bizarre weather is also consistent with a long-term trend. While summertime temperatures across the Antarctic Peninsula normally hover around freezing or rise just a few degrees above, the region has experienced dramatic warming in recent decades, making it easier for heat spells to veer into record-breaking territory. And with Earth's climate continuing to warm as atmospheric carbon levels soar, any newly minted records probably won't last long.

**Analyst Comment:** Toward the beginning of February, high-pressure air migrated over South America's southern tip, enveloping the region in warm weather. Normally, the effects of this aren't felt on the Antarctic Peninsula, as a belt of strong winds encircling the continent protects it from warm air incursions. But in recent months, these winds have been in a weakened state around the South Pole, part of a recurring pattern known as the Antarctic Oscillation. Additionally, ocean temperatures surrounding the northern tip of the Antarctic Peninsula were 3-5°F warmer than usual toward the beginning of the month.

On 06 February, an Antarctic base recorded a temperature of 65°F, beating the station's previous high record of 63.5°F (March 2015), which also stands as the all-time high temperature record for the entire continent. Then, on 9 February, another research station logged 69.4°F, according to several media reports. If verified, it will be the highest ever temperature measurement not just for Antarctica, but for the entire region south of 60 degrees latitude.

While Antarctica as a whole has only warmed slightly since the mid-20th century, at long-term research stations on the Antarctic Peninsula, temperatures rose 5°F between the 1950s and the early 2000s, far outpacing the globally averaged rate of warming. Then, in the late 1990s, this rapid warming abruptly stalled. Still, scientists expect the peninsula will start to heat up again in the not-so-distant future. As the region heats up, polar ice will weaken and melt, affecting oceans across the globe.

Source: <https://www.nationalgeographic.com/science/2020/02/antarctic-peninsula-setting-heat-records-wont-stand-long/#close>



## DoD Installations May Serve as Coronavirus Quarantine Sites – *Biological Hazards*

**Excerpt:** Four U.S. bases are on standby to assist the Department of Health and Human Services with housing those fleeing the novel coronavirus threat, Pentagon officials said Saturday.

Defense Secretary Mark Esper approved an HHS request Saturday to house 1,000 people who may require quarantine following overseas travel, according to a Defense Department statement.

"HHS officials requested the Defense Department to provide several facilities capable of housing at least 250 people in individual rooms through Feb. 29, 2020," officials said.

Tapped for the contingency were The 168th Regiment, Regional Training Institute, in Fort Carson, Colorado; Travis Air Force Base, California; Lackland Air Force Base, Texas; and Marine Corps Air Station Miramar, California.

**Analyst Comment:** The selection of DoD installations for potential use as COVID-19 novel coronavirus quarantine sites comes as concerns regarding the emerging disease rise among widespread infections and deaths worldwide. DoD installations are uniquely equipped to handle the quarantine of large numbers of individuals due to their secure nature and ability to provide housing for large numbers of individuals. However, a DoD statement stated that DoD personnel will not be directly in contact with those who are quarantined, and quarantined individuals will not have any access to areas of installations except for their assigned housing units. Medical care, transportation, and security is to be provided by the Department of Health and Human Services (HHS) in the event that DoD installations are utilized. This arrangement between DoD and HHS is similar to what was proposed in 2018 when DoD installations were identified to provide support to immigration agencies conducting migrant detention operations.

Source: <https://www.military.com/daily-news/2020/02/01/4-more-military-bases-tapped-house-coronavirus-evacuees.html>

---

## Locust Outbreak in East Africa – *Biological Hazards*

**Excerpt:** The worst locust outbreak that parts of East Africa have seen in 70 years has reached South Sudan, a country where roughly half the population already faces hunger after years of civil war, officials announced.

Around 2,000 locusts were spotted inside the country, Agriculture Minister Onyoti Adigo told reporters. Authorities will try to control the outbreak, he added.

The locusts have been seen in Eastern Equatoria state near the borders with Ethiopia, Kenya and Uganda. All have been affected by the outbreak that has been influenced by the changing climate in the region.





The situation in those three countries “remains extremely alarming,” the U.N. Food and Agriculture Organization said in its latest Locust Watch update. Locusts also have reached Sudan, Eritrea, Tanzania and more recently Uganda.

**Analyst Comment:** Desert locusts - whose destructive infestations cause large-scale crop damage and hunger - are a species of grasshopper that live largely solitary lives until a combination of conditions promote breeding and lead them to form massive swarms. The locusts have led to what the Food and Agriculture Organization has called the "worst situation in 25 years" in the Horn of Africa. There have been six major desert locust plagues in the 1900s, the last of which was in 1987-89. The last significant surge was in 2003-05.

Somalia has declared a national emergency due to the outbreak. The first wave of locust swarms last December destroyed about 100,000 hectares of farmland and pastures there. This wave of locusts has been traveling for several months. The eggs laid will likely hatch at the beginning of the rainy season in April. Then, the number of overall locusts could grow up to 500 times. More rains in the coming weeks will most likely bring fresh vegetation to feed a new generation of the voracious insects.

The locusts have traveled across the region in swarms the size of major cities. Experts say their only effective control is aerial spraying with pesticides, but U.N. and local authorities have said more aircraft and pesticides are required. A handful of planes have been active in Kenya and Ethiopia.

Food scarcity across several countries will likely impact local infrastructure and vulnerable populations. There is the potential for civil disturbance activity or mass migration as the situation worsens.

*Source:* <https://abcnews.go.com/International/wireStory/huge-locust-outbreak-east-africa-reaches-south-sudan-69048002>

---

## **U.S. Nuclear Waste May Be Stored Unsafely – *Accidental Events***

**Excerpt:** The current model the U.S. and other countries plan to use to store high-level nuclear waste may not be as safe as previously thought.

The materials used to store the waste "will likely degrade faster than anyone previously knew" because of the way the materials interact, according to research published Tuesday [27 January] in the journal Nature Materials.

The research, funded by the U.S. Department of Energy Office of Science, focused primarily on defense waste, the legacy of past nuclear arms production, which is highly radioactive, according to a press release from Ohio State University. Some of waste has a half-life -- the time needed for half the material to decay -- of about 30 years. But others, such as plutonium, have a half-life that can be in the tens of thousands of years, according to the release.



The plan the U.S. has for the waste is to immobilize long-lived radionuclides -- mixed with other materials to form glass or ceramic forms of the waste -- in steel canisters and then dispose of them by burying them in a repository deep underground, according to the study. Countries around the globe largely store and dispose of the nuclear waste in a similar fashion.

**Analyst Comment:** In this study, scientists found that under simulated conditions, corrosion of the containers could be "significantly accelerated," which had not been considered in current safety and performance assessment models. The steel cannisters, filled with glass and ceramic forms of waste, are corroding at unexpected rates due to new chemical reactions.

The problem was identified when pieces of stainless steel were pressed against glass or ceramic and submerged in a saltwater solution, simulating groundwater exposure. When water seeped into the boundary between the stainless steel and ceramic or glass, the steel released ferrous iron, ferric iron and other components that created an acidic environment at the metal's surface. That acidity corroded the neighboring ceramic or glass.

These storage sites may require reassessment regarding the security and longevity of waste storage, particularly in relation to groundwater exposure. It should be noted that nuclear waste is typically stored where it is produced. While the EPA proposed that the waste be disposed in a deep geological repository in Nevada, the plans have been stalled since 2009.

*Source:* <https://abcnews.go.com/International/current-model-storing-nuclear-waste-sufficiently-safe-study/story?id=68584067>

---