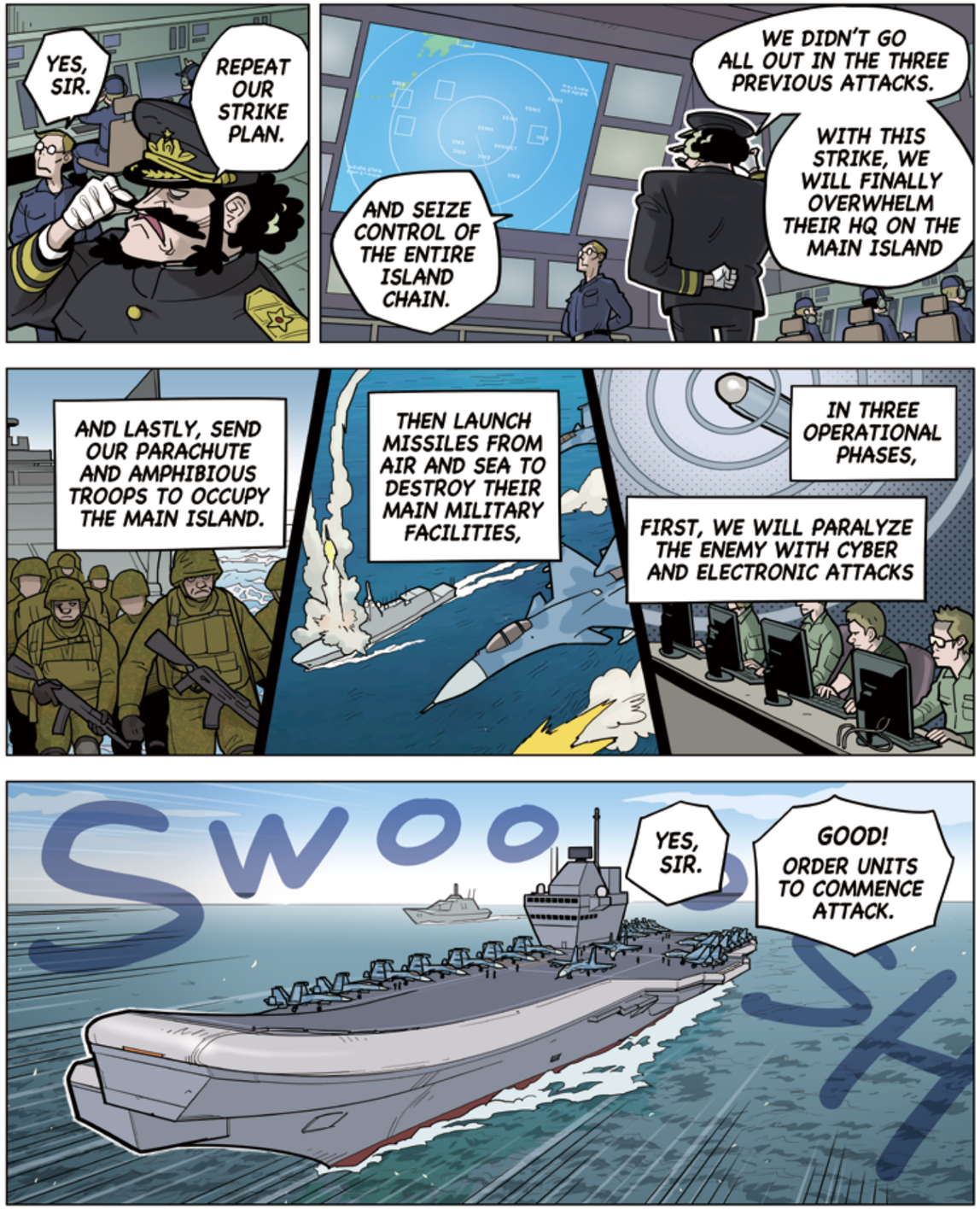
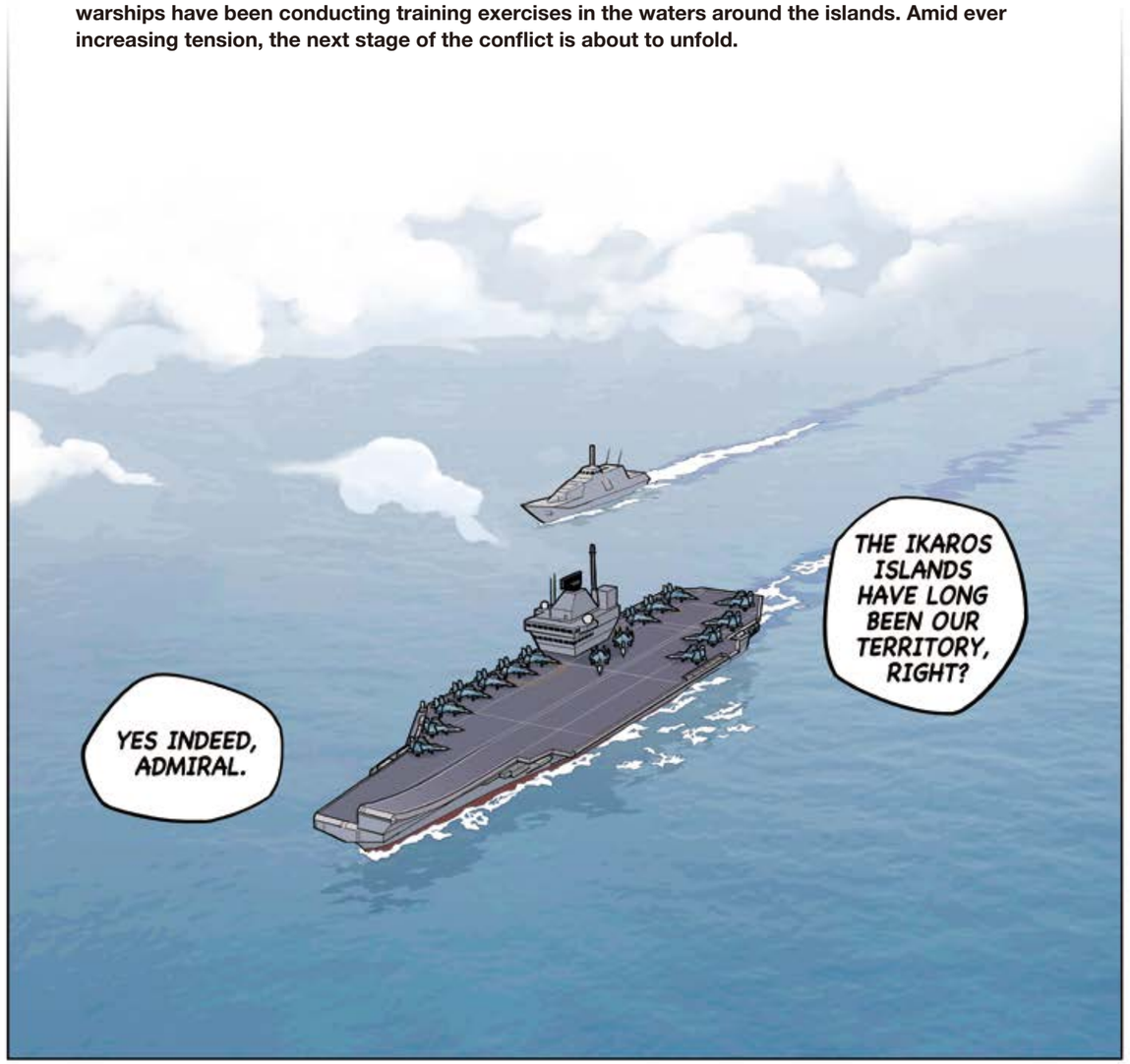
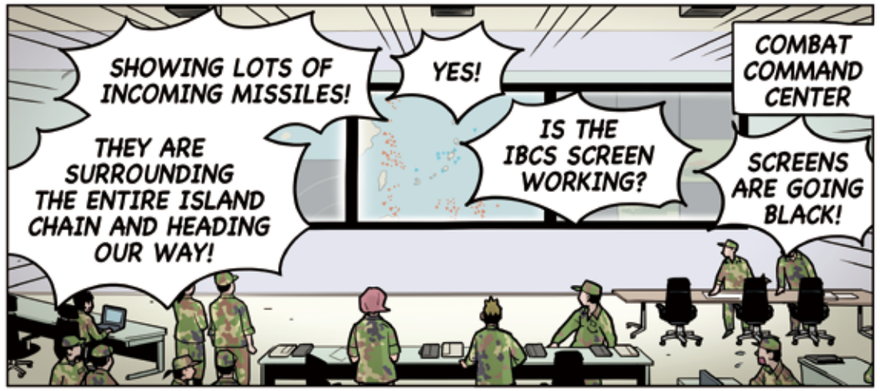


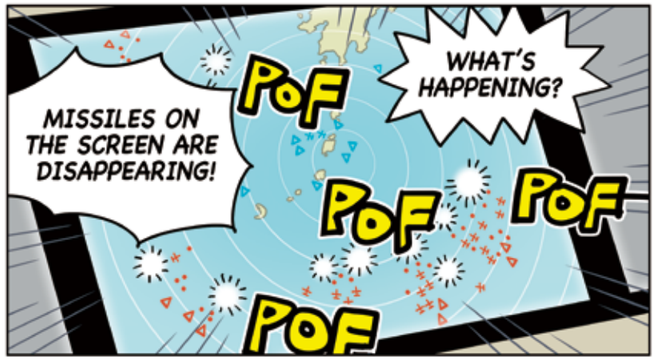
Episode 4:

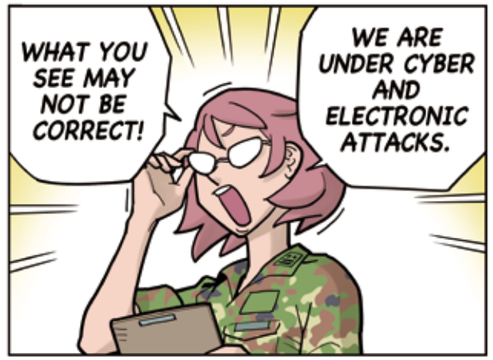
An Invisible Enemy: Cyber and Electronic Warfare

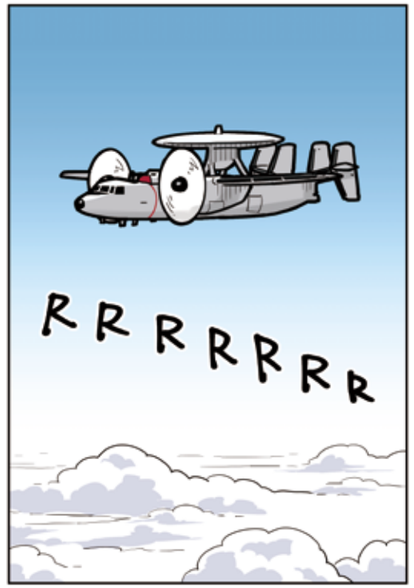
The nationality of the aircraft that launched the hypersonic missile has been identified. Despite diplomatic pressure, the country concerned dismissed the missile launch as "accidental." But what's actually happening is something completely different. An increasing number of that country's warships have been conducting training exercises in the waters around the islands. Amid ever increasing tension, the next stage of the conflict is about to unfold.

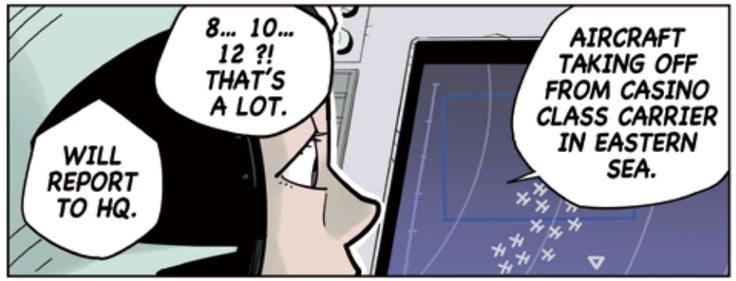




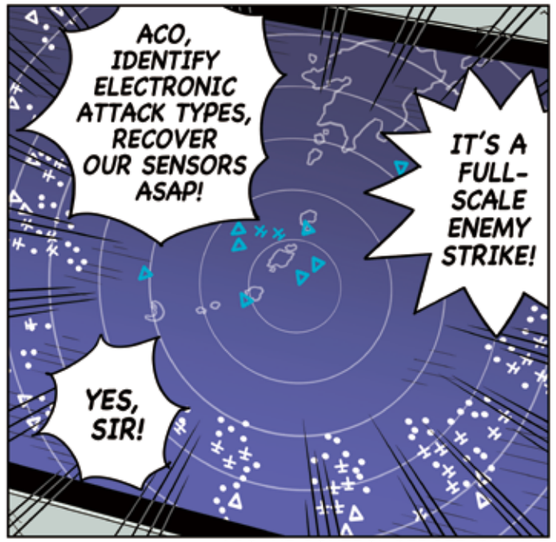


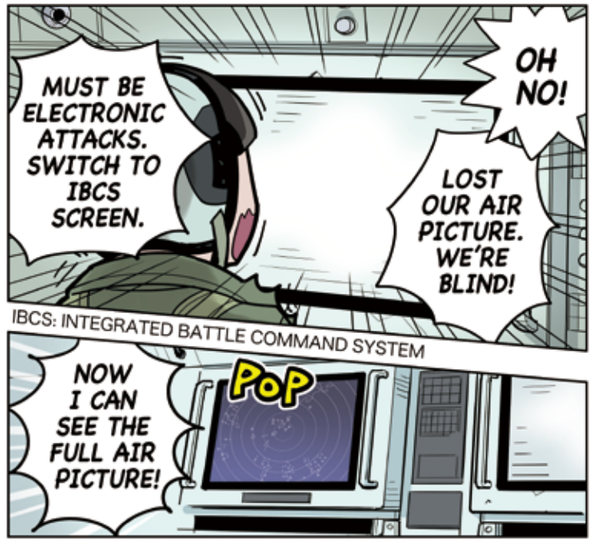






CAP: COMBAT AIR PATROL





IBCS: INTEGRATED BATTLE COMMAND SYSTEM

ACO: AIR CONTROL OFFICER. ON AN E-2D, THE COMBAT INFORMATION CENTER OFFICER (CICO), ACO, AND RADAR OFFICER (RO) DIVIDE RESPONSIBILITIES FOR AEW&C OPERATIONS.

IBCS

Resilient against cyber and electronic attacks

IBCS's world-class resilience

In Episode 4, the attacker finally launched the full-scale strike they should have done from the start. The strike operation in this episode is conducted in the standard sequence of modern warfare: start with cyber and electronic attacks, secure air superiority, then land ground combatants to control the island. However, it looks like both cyber and electronic attacks achieved only limited results, being stymied by IBCS.

Cyber Warfare and Electronic Warfare Are Different

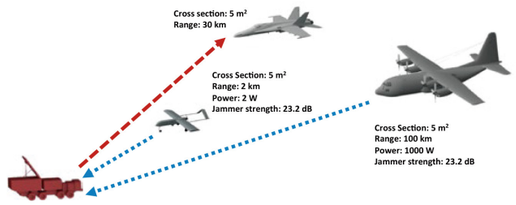
Recently, cyber warfare and electronic warfare are often lumped together. There are some commonalities, in that both aim to reduce or neutralize the capabilities of sensors or information communication and command and control systems. However, it is important to note that the targets and methods of each are completely different.

Electronic warfare primarily targets radio emission equipment such as radar and wireless communications. Both equipment types use radio waves; the difference lies in whether they are used for detection or communication. Electronic warfare is characterized by seeking to direct manipulate radio waves to disrupt enemy operations.

For instance, in the case of radar, one means of disruption is to make it impossible to receive reflected waves required for detection by emitting powerful jamming waves against the targeted radar. Another method is to generate fake detection targets by emitting false reflected waves at a different timing than the original reflected waves or from a different direction (as depicted in this episode). Communication could also be rendered impossible by sending strong jamming radio waves.

(Photo Credit: U.S. Navy)

FIGURE 15: JAM-TO-SIGNAL POWER POSSIBLE WITH DIFFERENT JAMMERS AT VARIOUS RANGES



Cyberattack, on the other hand, primarily targets computer systems and the data exchanged among them. Commonly used methods include interfering with computer systems' operations, overloading them, stealing data, or sending fake data.

Using the analogy of a postal service, electronic warfare can be thought of as interfering with the delivery of mail itself, while cyber warfare involves secretly switching or rewriting the contents of the mail.

An actor can also interrupt wireless communications by inserting phony communications. This method was used by the British military against the German air defense during World War II, which by attack method and approach may be said to be like a cyberattack.

The underlying requirement remains that radio weapons/equipment, communication systems, and computer systems (including, of course, command and control systems such as IBCS) in modern warfare must be hardened against electronic and cyber warfare.

Cyber and Electronic Attacks in This Episode

In this episode, the attacker first conducted cyber and electronic attacks to cripple the defender's interceptor systems.

A cyberattack is an attack against an adversary's system through a communication network of electronic terminals. Methods include data attacks that cause malfunction or overload the opponent's system, software attacks (e.g. 'Trojan Horse', worm) that cause malfunctions when inserted into the opponent's system, and hacking that directly enters the opponent's system to sabotage, take over, or steal data. In this episode, the attacker partly succeeded in disrupting the defender's systems.

Electronic attack aims to degrade or neutralize an adversary's communications equipment and radar by transmitting powerful or deceptive radio waves. In this episode, jamming caused communication problems and successfully blinded some radars.

When conducting electronic attack, the attacker needs to position a device that can transmit powerful radio waves at a location where the radio waves can reach the target. For this purpose, highly mobile aircraft are often used. The figure below, taken from a report by the Center for Strategy and Budgetary Assessments (CSBA), shows a stand-off jamming attack from a distance by a large device onboard a larger aircraft (stand-off jams) and a close-range jamming attack by an unmanned aircraft (stand-in jams) to be equally effective.

Electronic-warfare aircraft

U.S. Air Force's EC-130 Compass Call electronic warfare aircraft. The large aircraft conducts various electric attacks with its large onboard equipment. (Photo Credit: U.S. Air Force)

U.S. Navy's EA-18G Growler. The aircraft conducts various electronic attacks with the EW pods attached beneath the fuselage and at the wingtips. (Photo Credit: U.S. Navy)

PLA's Y-9 electronic warfare aircraft. It is estimated that China's electronic warfare capabilities have already reached a high level. It has also produced an electronic warfare variant of the J-15 fighter. (Photo Credit: Japan's Joint Staff Office)

U.S. Marine Corps' RQ-7 Shadow UAV. Though having retired by the Marines in 2018, the tactical UAV's concept was to approach the enemy close to conduct electronic attacks while reducing human risk.

Why can IBCS Discard False Target Information?

As explained in previous episodes, IBCS generates a single situational picture by networking multiple sensors (such as radars) and fusing the data gathered from them. Even if some of those sensors were disrupted by electronic attack, IBCS can compare information from sensors that have not been jammed to determine which one is a false target.

For instance, suppose radar A detects 20 targets in a certain airspace, while radar B detects 50 targets. Where does the difference in number of detected targets come from? If it can be determined that radar B is detecting false targets because of electronic attack or that the radar's information processing has been disrupted by cyberattack, we can conclude that radar A is normal. Then, by utilizing information from radar A, the false detections by radar B can be discarded.

This is only possible by networking multiple sensors and fusing their data.

Electronic warfare affects communications as well as radar. To counter electronic attacks targeting communications, wireless communication technology that is resilient to the attacks is necessary. In fact, wireless LAN and Bluetooth use similar technologies. Instead of communicating within a specific narrow frequency range, they "dilute" the communication to a wider frequency range, or frequently change the frequencies they use. Of course, in the latter case, parties on both sides of the communication must synchronize and convert the frequencies for communication to succeed.

In developing IBCS, tests were conducted under conditions assuming electric attacks. However, when it comes to the question of how IBCS specifically responds to electronic attack by an enemy, this is the most sensitive part that cannot be made public. Therefore, it can't be helped that the manufacturer can't say much. Here, I'll simply write that IBCS has a proven track record of functioning properly in tests conducted under highly contested electronic warfare environments.

A Cyberattack-Resilient System

In this article, I explained what to do in case an electronic attack has deceived the system into detecting false targets. There could be a situation in which a cyberattack could do the same thing, but in such a case, the method would be different.

First, an attack program must be sent to the computer that performs radar signal processing (analyzing the reflected waves received by the antenna and calculating the position, course, and speed of the detected target) and executed. The program then "hijacks" the computer's signal processing function and creates targets that do not actually exist.

To counter such attacks, the defender must have functions to not allow such malicious programs to be inserted in the first place and promptly recognize the presence of such a program and eliminate it. This is similar to running anti-virus software on PCs and smartphones.

Again, the details of how cyberattacks are handled by IBCS are strictly confidential. However, it is widely known that U.S. weapon systems including IBCS are designed, developed, and tested against various types of cyberattacks.

In addition, multiple command posts, called EOC (Engagement Operations Center), can be established within the IBCS network. This has the benefit that if any EOC is destroyed, other EOCs can continue operations—and the destruction doesn't have to be physical. What if a cyberattack were to cause disruption to a specific EOC? In such a case, as long as there are multiple EOC, those still-functioning EOC can continue operations.