ALERTEX 2018-B PRE-EXERCISE TRAINING
15-18 August 2018

ALERTEX 2018-C is a black sky exercise based on a significant cyber-attack on national and international electrical power and Internet systems. This exercise is preparation for REACT International's participation in EARTH EX 2018, a major international black sky exercise on 22 August 2018.

Objectives

The objectives for ALERTEX 2018-C are:

(1) Determine the capability of REACT Teams to operate under sustained power and Internet outages to support the organizations with which they have memoranda of agreement.

(2) Identify areas in which REACT International can realistically increase its capability to communicate in an extended power outage event.

Chronology

The following is a timeline of some (and we emphasize some) of the known cyberattacks that caused significant disruption, damage, and loss:

Year	Where	What Happened	Impact
2000	Australia	Disgruntled computer expert gains control of waste water system 46 times	Hundreds of thousands of gallons of raw sewage spilled in parks, rivers, public areas
2013	New York	7 Iranians gained control of dam controls in Rye Brook and also attacked 45 financial institutions	
2014	Worldwide	Reported 160,000 attacks on power distribution systems	
2015	Ukraine	Russian attack on an electric power distribution system	230,000 to 700,000 without power for 2 hours

2016	United States	3 waves of Distributed Denial of Service attacks on Dyn, a major control system for Internet operations by "friends of Wiki-Leaks"	2 hours outages to major Internet users
2016	United States	Russian military intelligence hacking attacks on local election boards, political candidates, and political organizations.	Voter lists stolen, e-mails and other documents stolen and released through Wiki-Leaks to influence the election against Democratic Party candidates.
Recent	Kansas	Nuclear power station controls attacked at a Kansas power station and at others	
2018	Denver, Colorado	Colorado Department of Transportation attacked by ransomware	After 6 weeks recovery was at 80%, cost $1.5 million to taxpayers
2018	Atlanta, Georgia	Ransomware attack on city government	Computer services out, widespread destruction of 16+ years of city records, after 9 days recovery only partial
2018	Worldwide	Computer security experts forecast sustained worldwide computer and electric power system outages, not if, but when	

Infrastructure at Risk

Infrastructure in simple terms is the man-built structures and systems that allow modern civilization to function. Much of the nation's infrastructure is vulnerable to disruption, or even destruction, from large scale power outages or from cyber-attacks on computer systems. This includes:

Electric Power – generation plants, including nuclear plants, distribution systems, transmission lines.

Communications – telephone, cellular telephone, pagers, radio, television, the Internet.

Transportation – air traffic control, airports, aircraft, highways, canals and locks, oil and gas pipelines, maritime traffic control centers, port facilities, canals, railroad dispatch centers, traffic control signaling.

Water – potable water distribution systems, wastewater systems, dams, irrigation systems, flood control systems.

Key Facilities – hospitals, public works and transportation department dispatching, key governmental facilities, prisons, metal health facilities, state (National Guard) and national military facilities.

Emergency Services – public access for emergency calls (911 as an example), dispatch systems, emergency operations centers, search and rescue centers.

Industrial – plants manufacturing hazardous materials, refineries.

The Black Sky Scenario

A well-designed attack on the computer systems vital to how our infrastructure works could cause accidents, kill people, result in the release of hazardous materials, cause significant financial losses, and take hours, days, weeks, or months for a complete return to normalcy. So far attacks on computer systems and infrastructure have been limited in scope and generally contained by current cyber-defenses. However, there is a very real possibility that what we have seen so far is probing to determine the system vulnerabilities of the United States and European countries.

The Black Sky scenario considers such an attack. So far we have seen:

(1) hacking to access and steal electronic records and information,

(2) denial of service attacks to overwhelm individual sites and portions of the Internet,

(3) ransomware attacks to seize vital records and hold them for ransom with the potential for those records never to be returned or to be returned corrupted, and

(4) direct attacks on control systems that have the potential to cause massive infrastructure failures.

(5) attacks conducted as a single attack or in waves of attacks.

(6) attacks by terrorists, criminal hackers, and hostile nations.

The larger and wider scale the attacks, the more stressed our limited national resources will be for response and recovery. This means that outages and associated impacts of 2 hours at the low end to months or even a year or more are a realistic possibility.

Impacts may be restricted to electrical power and computer systems, but in the case of widespread failures a whole range of secondary failures may occur. For example, an outage to electrical power in a facility that requires power to safely store hazardous materials may result in a fire and explosion. At the same time the loss of power to reverse 9-1-1 systems, and television and radio stations may mean that evacuation orders downwind will be delayed leading to exposures of large number s of people to toxic gases. The hospitals to which those patients are taken may also be impacted by power and communications outages leading to increased fatality counts.

We do not know how such an attack would be made by a determined terrorist organization or a hostile nation. However, there are two obvious scenarios:

(1) an attack that starts with minor, seemingly unconnected incidents, that consume resources and cause disruption. These may be targeted at specific vital infrastructure or at targets that have the greatest secondary impacts. If these incidents cause significant secondary impacts, they may be sufficient to meet the attacker's objectives, or they may be the first stage of …

(2) a massive attack on the electrical power and communications systems of the country. Disabling these two closely related infrastructure sectors would likely cause related widespread cascading failures in other infrastructure that would extend well beyond the targeted country or countries.

Operating Assumptions

REACT communications in such an event would depend upon available back-up power sources for radio communications, including battery, generator, wind, or solar power.

Repeaters that do not have back-up power will be unavailable.

Battery back-up systems will fail at some time based on the typical life of the battery without recharging. Resupply beyond your stockpile of batteries will not be possible.

Generators will fail when fuel supplies are exhausted. Resupply of fuel, including for vehicles, will not be available.

Internet communications will be unavailable or will be severely degraded with transitory or long-term outages.

Alerting Team members and coordination with supported organizations and other REACT Teams will be far more difficult than in normal emergencies.

As a minimum, outages will last hours. At a maximum, weeks to months.

Preparing for Outages

It is to your Team's advantage to work to develop a capability to operate for as long as possible without electricity and without telephone and computer communications. This requires a layered approach.

First – protect your computers: Increasingly we have computers everywhere in our lives. If you have a new refrigerator or a home security system, you may well have a computer that is vulnerable to being used by hostile forces. It is not just your desktop or laptop or tablet. Protecting computers from hacking, malware attacks, or from being used surreptitiously as part of large denial of service attacks requires:

- Good procedures – (1) avoid opening e-mails and especially attachments that you do not recognize or expect, (2) ensure your privacy settings are appropriate for your use, (3) avoid websites that trigger security warnings, (4) do not leave your computer on when it is not in use, (5) ensure programs have current software updates, (6) do not use thumb drives or other storage media that have been in other peoples' computers.

- Good anti-virus, anti-malware, anti-ransomware software – (1) have a complete security suite, (2) ensure that it is updating regularly, (3) ensure the settings selected provide appropriate security.

- LAN security – ensure that you use an encrypted local area network.

Second – broaden your communications capabilities: To sustain communications you must have the capability to operate with radios that cover a wide area. This may be as short a wide area as from your neighborhood to the emergency operations center. It may be that you have to have the capability to use a radio link to contact an amateur radio station that can access national traffic nets. Remember that communications failures may impact only some means of communications. Increase your capabilities by being able to operate on as many as possible.

- If you rely on one radio system, especially one that cannot talk to the public or to an amateur radio station, get one or more other radios that operate on services that can receive reports from the general public and that can interface with the amateur radio system.

- If you have a radio that can talk to a variety of users, upgrade. Get a better antenna. If you have an AM CB radio get a SSB radio. If you operate with a handheld radio, get a mobile or base station.

- If you rely on a repeater, make sure that the repeater you use can sustain commercial power outages. Talk to the repeater owner and understand what his or her plan is for a major outage.

- If you rely on Echolink or Winlink, remember that they are no more sustainable than your computer is. Develop a high frequency amateur capability.

- Get to know the other voluntary emergency communications organizations in your community – you may need their help, or they may need yours.

- If you rely on Zello through your computer, get a network radio – if the cell phone systems are operational, you will be able to operate.

- If you have members who use alphanumeric pagers, make sure you know their pager e-mail addresses and test communications with them regularly.

Third – get a capability to operate without electricity: This means you should explore:

- Batteries – batteries are a short term solution, hours to days. If your radio can be powered by standard commercial batteries, you will need a significant stockpile. That also means you need to rotate the stock, using older batteries and replacing them with new ones. Rechargeable batteries require that you manage recharging according to the specific characteristics of the battery.

- Generators – generators are a short-term solution governed by the fuel supply, typically days. In a major black-sky event the ability to refuel will rapidly go away with the failure of electric power.

- Other power sources – the most accessible and portable of these is probably solar panels to recharge batteries, although wind power generators are also available. These renewable energy approaches are probably capable of longer operation, although the power they output must be matched to the requirements of your radios.