Question: 18. Should a CBDC have “offline” capabilities? If so, how might that be achieved?

Return to Design Considerations | **Provide Feedback**

Question

Return to Top

1. **Should a CBDC have “offline” capabilities?**
2. **If so, how might that be achieved?**

Answer

Return to Top

The answer is yes.

Overview

Return to Top

At the heart of this problem are Disconnected, Intermittent, and Limited (DIL) links.

> *Disconnected, Intermittent, and Limited (DIL) occur in wireless/mobile networking environments, e.g. rural area networks, vehicular networks, battlefield networks, and other resource-constrained or disadvantaged networks. Efficient and effective interoperability in these networks are highly demanded various mission-critical systems and application scenarios such as disaster relief in ravaged regions, search and rescue in remote areas and military/tactical operations in hostile environments. (DIDO-RA and IEEE)*

A DIL can occur whenever a network becomes unavailable. The definition of a DIL elaborates on three cases: disaster relief in ravaged regions, search and rescue in remote areas, and military/tactical operations in hostile environments. A fourth case, Network Outages is added to highlight just how fragile the reliance on networks can be.

Table 1: Situations where Disconnected, Intermittent and Limited (DIL) occur and have an impact on CBDC.

Situation	Description
Disaster relief in ravaged regions	FEMA Led Historic Pandemic Response, Supported Record Number of Disasters in 2020 1. FEMA responded to the most active Atlantic hurricane season in history. More than 5,000 FEMA employees deployed to support both Atlantic and Pacific hurricane responses in 2020. 2. 2020 saw 30 record named storms, with the previous record of 27 named storms in the 2005 hurricane season. a. Twelve of these storms made landfall in the U.S., surpassing the 1916 record of nine storms making landfall in the U.S. b. September 2020 set a record with 10 named storm formations. On Sept. 18, three Atlantic storms formed within six hours, which previously occurred only one other time in 1893. 3. Five of the named storms made landfall in Louisiana. a. As of Jan. 4, 2021, FEMA has provided over \$245 million in grants and \$1.2 million in flood policy payments to survivors in Louisiana. b. FEMA also provided more than \$2.3 million in grants to governments and nonprofits to assist with response efforts and rebuild infrastructure. 4. FEMA responded to the most active West Coast wildfire season on record. More than 1,200 employees were deployed to support the response to western wildfires. a. These included the largest wildfire in Colorado's recorded history, the Cameron Peak fire, and five of the 10 largest fires in California's history. 5. FEMA processed three major declarations due to wildfires.
Search and rescue in remote areas	While the nation continues to make progress in broadband deployment, millions of Americans still lack access to adequate broadband, especially in rural areas and on Tribal lands. This baseline map visualizes broadband access at the county level and identifies connectivity gaps — the lighter the color, the lower the percentage of households with broadband access. Broadband Gaps in the USA Figure 1: Broadband coveragein the USA **Note:** This does not include "at sea" coverage

Situation	Description
Military/tactical operations in hostile environments	Communication with submarines is a field within military communications that presents technical challenges and requires specialized technology. Because radio waves do not travel well through good electrical conductors like saltwater, submerged submarines are cut off from radio communication with their command authorities at ordinary radio frequencies. Submarines can surface and raise an antenna above the sea level, then use ordinary radio transmissions, however, this makes them vulnerable to detection by anti-submarine warfare forces. Early submarines during World War II mostly traveled on the surface because of their limited underwater speed and endurance; they dived mainly to evade immediate threats. During the Cold War, however, nuclear-powered submarines were developed that could stay submerged for months. In the event of a nuclear war, submerged ballistic missile submarines have to be ordered quickly to launch their missiles. Transmitting messages to these submarines is an active area of research. Very low frequency (VLF) radio waves can penetrate seawater a few hundred feet (10–40 meters), and many navies use powerful shore VLF transmitters for submarine communications. A few nations have built transmitters that use extremely low frequency (ELF) radio waves, which can penetrate seawater to reach submarines at operating depths, but these require huge antennas. Other techniques that have been used include sonar and blue lasers.
Network Outages	Wikipedia has identified 19 major internet outages (see Table 1 that have occurred because of hardware or cabling, internet infrastructure, cyber-attacks, government censorship, and server overloads.

Many of these problems create a situation often referred to as the Two Generals Problem which for the most part is unsolvable. However, if each general can work independently of the other (i.e., disconnected or offline), then the number of occurrences of the **Two Generals Problem** is reduced.

> **Note:** The Two Generals is related to, but distinct from Byzantine General Problem. The Two Generals problem is about the weakness in the connectivity between the Generals. The Byzantine General Problem is about the weakness of a General.

Table 1: List of Internet outages provided by Wikipedia.

Year	Name	Country or region	Affected users	Number of affected users (rough)	Description	Duration (rough)	Internet component	Cause	Entity responsible	Type
16 Jul 1997	DNS TLD Outage	Worldwide		50,000,000	An Ingress database failure resulted in corrupt .com and .net zones, which were subsequently released to the DNS root servers. As the root servers were reloaded, they began to return failures for all domains in the .com and .net zones.	4 hours	DNS	Automation and Human Failure	InterNIC / Network Solutions	All .com and .net domains

Year	Name	Country or region	Affected users	Number of affected users (rough)	Description	Duration (rough)	Internet component	Cause	Entity responsible	Type
2008	2008 submarine cable disruption	Middle East and the Mediterranean Sea			Three separate incidents of major damage to submarine optical communication cables around the world occurred in 2008. The first incident caused damage involving up to five high-speed Internet submarine communications cables in the Mediterranean Sea and the Middle East from 23 January to 4 February 2008, causing internet disruptions and slowdowns for users in the Middle East and India. In late February there was another outage, this time affecting a fiber optic connection between Singapore and Jakarta. On 19 December, FLAG FEA, GO-1, SEA-ME-WE 3, and SEA-ME-WE 4 were all cut.		submarine cables	Unknown	Unknown	
2011	2011 submarine cable disruption	South Asia and the Middle East			Two incidents of submarine communications cables cut off on 25 December 2011. The first cut-off occurred to SEA-ME-WE 3 at Suez Canal, Egypt and the second cut-off occurred to i2i which took place between Chennai, India, and Singapore line. Both the incidents had caused Internet disruptions and slowdowns for users in South Asia and the Middle East in particular UAE.	submarine cables	Unknown	Unknown		
2011		Armenia		3,000,000	A woman digging for scrap metal damaged land cables and thereby severed most connectivity for the nation of Armenia.	5 hours	land cables	digging		Full

Year	Name	Country or region	Affected users	Number of affected users (rough)	Description	Duration (rough)	Internet component	Cause	Entity responsible	Type
2011		Egypt			The Internet in Egypt was shut down by the government, whereby approximately 93% of networks were without access in 2011 in an attempt to stop mobilization for anti-government protests.		ISPs	government censorship	Egypt	Full
2012		2012 Syrian internet outage	Syria		On 29 November 2012, the Syrian Internet was cut off from the rest of the world. The autonomous system (AS29386) of the Syrian Telecommunication Establishment (STE) was cut off completely at 10:26 UTC. Five prefixes were reported to have remained up, this is why Dyn reports an outage in 92% of the country. Responsibility for the outage has somewhat speculatively been blamed on various organizations.			Unknown	Unknown	
2016		Germany	Deutsche Telekom	900,000	At the end of November 2016 0.9 million routers, from Deutsche Telekom and produced by Arcadyan, were crashed due to failed TR-064 exploitation attempts by a variant of Mirai, which resulted in Internet connectivity problems for the users of these devices. While TalkTalk later patched their routers, a new variant of Mirai was discovered in TalkTalk routers.	1 day	Internet routers	cyberattack	Unknown	Full

Year	Name	Country or region	Affected users	Number of affected users (rough)	Description	Duration (rough)	Internet component	Cause	Entity responsible	Type
2016		Liberia		Unknown	Mirai has also been used in an attack on Liberia's Internet infrastructure in November 2016.			cyberattack	Unknown	Full

Year	Name	Country or region	Affected users	Number of affected users (rough)	Description	Duration (rough)	Internet component	Cause	Entity responsible	Type
2016	DDoS attack on Dyn	United States	Dyn (company)		The cyberattack took place on October 21, 2016, and involved multiple distributed denial-of-service attacks (DDoS attacks) targeting systems operated by Domain Name System (DNS) provider Dyn, which caused major Internet platforms and services to be unavailable to large swathes of users in Europe and North America. As a DNS provider, Dyn provides to end-users the service of mapping an Internet domain name—when, for instance, entered into a web browser—to its corresponding IP address. The distributed denial-of-service (DDoS) attack was accomplished through a large number of DNS lookup requests from tens of millions of IP addresses. The activities are believed to have been executed through a botnet consisting of a large number of Internet-connected devices—such as printers, IP cameras, residential gateways and baby monitors—that had been infected with the Mirai malware. With an estimated throughput of 1.2 terabits per second, the attack is, according to experts, the largest DDoS attack on record.	1 day	Domain Name System (DNS) provider	cyberattack	Unknown	Major websites

Year	Name	Country or region	Affected users	Number of affected users (rough)	Description	Duration (rough)	Internet component	Cause	Entity responsible	Type
2017		Cameroon	South-West and North-West of Cameroon	20% of the country's population	On January 17, around 20 percent of the people in Cameroon had their Internet blocked due to recent anti-government protests.	270 days or 8 months		government censorship	Cameroon	Full
2017		North Korea			On October 1, The autonomous system (AS131279) of Star JV was cut off completely, due to alleged US cyber attack	9 hours and 31 minutes		cyberattack	United States	Full
2019	Verizon and BGP Optimizer	United States	Verizon (company)		On June 24, 2019, many parts of the Internet faced an unprecedented outage as Verizon, the popular Internet transit provider accidentally rerouted IP packages after it wrongly accepted a network misconfiguration from a small ISP in Pennsylvania, USA. According to The Register, systems around the planet were automatically updated, and connections destined for Facebook, Cloudflare, and others, ended up going through DQE and Allegheny, which buckled under the strain, causing traffic to disappear into a black hole.	3 hours	Internet transit provider	misconfiguration	Unknown	Major websites
2019	Iranian internet shutdown	Iran			The Internet in Iran was shut down by the government, whereby approximately 96% of networks were without access in an attempt to stop mobilization for anti-government protests.	7 days	ISPs	government censorship	Iran	Full

Year	Name	Country or region	Affected users	Number of affected users (rough)	Description	Duration (rough)	Internet component	Cause	Entity responsible	Type
2019	Internet shutdown in India	India		50,000,000	The Government of India passed the Citizenship Amendment Act, 2019 which caused huge controversy and mass protest in various parts of India. In order to prevent protests and outrage on social media, various state governments including those of Assam, Tripura, Meghalaya, Arunachal Pradesh, West Bengal, and Uttar Pradesh decided to shut down internet access.	Up to 9 days Over one year (Kashmir)		government censorship	Various State governments of India	Full
2019	2019 Burmese internet shutdown	Myanmar			On June 21, the Internet in Burma was shut down by the government. The Burmese government shut down the internet connection in nine townships of the northern Arakan State and one single township in the Southern Chin State, which was proposed by Burmese Military officers. The shutdown is ongoing and has become the world's longest internet shutdown.			Government censorship	Burma	Full
2019	2019 Papua protests	Indonesia			To curb the escalating protests that occurred in the Indonesian provinces of Papua and West Papua, the Indonesian authority imposed an internet blackout on both provinces on 21 August 2019. The blackout continues until the authority partially lift the blackout on 4 September in several regions, with the complete lifting of the restriction only occurring on 9 September.	19 days		Government censorship	Indonesia	Full

Year	Name	Country or region	Affected users	Number of affected users (rough)	Description	Duration (rough)	Internet component	Cause	Entity responsible	Type
2021		North Korea			On October 21st, North Korean internet infrastructure dropped off the internet, including public-facing websites and email servers. All servers which were subject to monitoring were found to be offline.	At least 14 minutes		Unknown	Unknown	
2021	Facebook Outage	Worldwide	LAN Internet Connection	2,850,000,000	On October 4, 2021, at around 11:45 AM EST, the online social media site Facebook went down, as well as Facebook subsidiaries including Instagram and Whatsapp. Around 4:00 PM EST, people reported other sites were not working via Downdetector, including Gmail and Twitter, the latter possibly caused by Facebook users reporting the outage. The outage came less than a day after a whistleblower had been on 60 Minutes. For a short period of time, no Facebook employee could access the building to investigate the issue due to their “keycards not working.”. At around 6:30 PM EST, Facebook reported that all their sites were up. Facebook CEO Mark Zuckerberg lost around \$7B dollars after the outage. For more info, see 2021 Facebook outage	7 hours	LAN connection	BGP Withdrawal of IP Address (Facebook), Server overwhelming (other sites)	Unknown	Major websites

Year	Name	Country or region	Affected users	Number of affected users (rough)	Description	Duration (rough)	Internet component	Cause	Entity responsible	Type
2022	2022 Kazakhstan internet shutdown	Kazakhstan			On 4 January 2022 the Internet in Kazakhstan was shut down on account of anti-government protests against sudden energy price rises.[75]	5 days		Government censorship	Kazakhstan	mobile internet

Examples

Return to Top

Some of these Disconnected, Intermittent and Limited (DIL) requirements were alluded to in the White Paper, but not directly specified or defined. The Table 2 provides an example of cross-referencing the DIL Requirements to the Benefits, Policy Considerations, Risks and Design requirements identified in the White Paper Analysis done by the Object Management Group's CBDC WG.

Table 2: Example of mapping a subset of requirements identified during the White Paper Analysis conducted by the OMG's CBDC WG.

Topic	Requirements
Disaster relief in ravaged regions	B: B0008, B0010, B0013, B0014, B0024, B0030, B0035, B0036, B0039, B0040, B0043, B0044, B0053 P: P0023, P0026 R: R0011 D: D0016, D0017
Search and rescue in remote areas	D: D0016, D0017
Military/tactical operations in hostile environments	B: B0013, B0018, B0030, B0024, D: D0016, D0017, B0030
Network Outages	B: B0018, B0030, B0024 D: D0016, D0017
B = Benefit Considerations	
P = Policy Considerations	
R = Risk Considerations	
D = Design Considerations	

Discussion of Example

Return to Top

The benefit specified **B0030** and the design specified **D0017**:

B0030	**14**	Support benefit payments directly to citizens
B0039	**15**	Provide a programmable CBDC to deliver payments at certain times
D0017	**20**	Design should include digital payments in areas suffering from large disruption, such as natural disasters

B = Benefit Considerations
P = Policy Considerations
R = Risk Considerations
D = Design Considerations

Both of these can be mapped to **Disaster relief in ravaged regions**. When a disaster occurs **D0017**, the US government can provide disaster relief through the Federal Emergency Management Agency (FEMA). The relief is often in the form of loans with payments, generally made through the US Small Business Administration (SBA). The assistance loans can be for businesses of all sizes, homeowners, and renters. CBDC needs to provide the payments directly to the recipients (i.e., **B0030** of the loans since many of the physical facilities of the existing financial institutions have also been damaged.

In addition, FEMA can offer assistance for Temporary Housing Assistance, Lodging Expenses Reimbursement[1)], which are recurring expenses. **B0039** would allow these payments to be made on a schedule and perhaps be made directly to the landlords or programmed to allow recipients to transfer the money to the landlord but nowhere else.

When access to the Internet becomes a Disconnected, Intermittent and Limited (DIL), often a Peer-to-Peer (P2P) network can be very effective, especially when other Network Platforms are used instead of just Ethernet with nodes connected over Local Area Network (LAN) and/or a Wide Area Network (WAN) using a Traditional Network Device. For example:

- Bluetoth
- Zigbee
- Near-Field-Communication (NFC)

Consequently, it is important to identify the kinds of connections that are required to support the CBDC. Some examples are:

- Many contactless payments systems use Radio Frequency Identification (RFID) and NFC
- Many supply chains use RFID
- Many smart home efforts use WiFi and Zigbee
- Many automobiles use Bluetooth to connect phones, make queries, play music, etc.

Another alternative is to establish a Wireless Fidelity (Wi-Fi) LAN that has no or very limited access to the Internet but can be used to connect local devices together.

Regardless of how the CBDC nodes connect, the information that flows between the nodes must be secure (See: OMG DIDO-RA Secure Messaging for a set of Technical and \\de Facto Standards for secure messaging.

The OMG DIDO-RA provides a detailed discussion on Networks, and we recommend that this be used when formulating further requirements for the CBDC. Some topics covered in the OMG DIDO-RA are:

- Secure Messaging
- Transport
- Security

- Protocol
- Distribution Software

1)

https://www.fema.gov/assistance/individual/housing