

TO THE POINT OF FAILURE



Identifying Failure Points for Crisis Communications Systems

Leah Walker | Alexa Wehsener

About the Institute for Security and Technology

As new technologies present humanity with unprecedented capabilities, they can also pose unimagined risks to global security. The Institute for Security and Technology's (IST) mission is to bridge gaps between technology and policy leaders to help solve these emerging security problems together. Uniquely situated on the West Coast with deep ties to Washington, DC, we have the access and relationships to unite the best experts, at the right time, using the most powerful mechanisms.

Our portfolio is organized across three analytical pillars: Geopolitics of Technology, anticipating the positive and negative security effects of emerging, disruptive technologies on the international balance of power, within states, and between governments and industries; Innovation and Catastrophic Risk, providing deep technical and analytical expertise on technology-derived existential threats to society; and Future of Digital Security, examining the systemic security risks of societal dependence on digital technologies.

IST aims to forge crucial connections across industry, civil society, and government to solve emerging security risks before they make deleterious real-world impact. By leveraging our expertise and engaging our networks, we offer a unique problem-solving approach with a proven track record.

Table of Contents

About the Institute for Security and Technology	2
Executive Summary	4
The State of Communication Failures and Nuclear Risk	5
Reducing Risk by Preventing Failures	5
Identifying Types of Communication Failures	6
Operational Failures	7
Historical Operational Failures	8
Accidental Failures	9
Historical Accidental Failures	10
Adversarial Failures	11
Historical Intentional/Adversarial Failures	13
Institutional Failures	14
Historical Institutional Failures	15
Patching Points of Failure	16
Conclusion	17
Appendix 1: Points of Failure in Nuclear Crisis Communications	18

Acknowledgments:

This report was made possible by the German Federal Foreign Office. The research informing it was enabled by generous support from the Swiss Federal Department of Foreign Affairs and the German Federal Foreign Office supporting the Institute for Security and Technology's [CATALINK](#) initiative.

Pledger Designs Ltd provided design services.

Copyright November 2022. Institute for Security and Technology.

Executive Summary

Although most states agree that the need for nuclear risk reduction is more urgent than ever, the pathways to peace are elusive. Existing use of hotlines is wrought with political and technical failures. In some cases, nuclear weapons states may not even possess direct communication lines to their nuclear adversaries or allies. Geopolitical tensions are rising and could be exacerbated if the number of states possessing nuclear weapons or those existing under nuclear security umbrellas continue to grow.

Nuclear crisis communications and other diplomatic communication systems reduce nuclear risk by increasing transparency and predictability in state actions and intentions, while combating miscommunication. Failures in those communication systems can eliminate their ability to reduce risk, and may, in fact, increase the risk of war. This report assesses operational, adversarial, accidental, and institutional failure points in existing nuclear crisis communications. These existing points of failure are cemented by the increasing complexity of today’s strategic environment and the additional risks it creates for reliable crisis communication use.



OPERATIONAL FAILURES

Failures driven by breakdowns in the way in which communication systems are operated, maintained, repaired, and rehearsed



ADVERSARIAL FAILURES

Failures caused intentionally by adversarial actors interacting with the system



ACCIDENTAL FAILURES

Incidents of failure driven by unexpected, inadvertent breakdowns in the system, or unexpected, inadvertent events that impact the system



INSTITUTIONAL FAILURES

Failures driven by behaviors and procedures (or lack thereof) that inhibit the use of the system

Using the above framework for categorizing communication systems, the report will also investigate how historical examples of each category of failures have increased nuclear risk. Finally, this report highlights mechanisms which could be used to mitigate point of failure concerns and strengthen nuclear crisis communication channels.

The State of Communication Failures and Nuclear Risk

In a world where risks of nuclear war are increasing, crisis communications and other diplomatic communication systems are critical mechanisms for reducing nuclear risk. Powerful states are modernizing their nuclear arsenals and integrating new capabilities even as arms control is waning, and with it transparency and predictability in state intentions. These combined factors risk miscalculation and inadvertent escalation. Yet many existing crisis communication channels are susceptible to technical, diplomatic, and policy points of failure, all of which could impede or discourage use. In many instances, the secure technologies are so archaic that senior leaders use their cell phones to text each other on commercial messaging applications. Although these public-use channels are expedient in peacetime, they are vulnerable to compromises and market failures, and in a crisis may be disabled entirely beyond states' control.

Leader-to-leader communication systems, like the U.S.-Russia hotline, have a track record of reducing nuclear risks, even at times that arms control was infeasible. The relationship built between the United States and the Soviet Union, followed by the relationship with Russia, was made a more stable dyad by national risk reduction centers, hotlines, theater level communication systems, and other informal channels between high level military and political leaders.

Nor do crisis communications need to be used only as a result of an incident. Simply building a habit of use generates trust, provides adversaries and competitors with information that can ease ambiguity, and sets up a mechanism that is familiar in case of crisis. During the Syrian Civil War and the Russo-Ukrainian War, the United States and Russia set up [deconfliction lines](#) to reduce the risk of escalation and incidents between the two armed forces operating in close proximity. The set up and use of these lines meant that in the case of any serious incident both sides knew precisely how to contact each other.

Reducing Risk by Preventing Failures

Crisis communications only decrease nuclear risk so long as the systems they rely on do not fail. Mitigating crisis communication failures is a critical part of any risk reduction strategy. Not only does preventing communication systems failures decrease nuclear risk overall, the mechanisms of failure mitigation can themselves reduce risk by increasing familiarity with the system, encouraging interaction with counterparts (and providing practice in negotiations), familiarizing personnel and ranking leaders with the system, and showing commitment to the system and its objectives. Geopolitical factors related to waning arms control agreements, emerging technologies, and an era of increased strategic competition further increase the likelihood of nuclear crisis while decreasing the likelihood that traditional nuclear hotlines will perform under pressure.

Identifying Types of Communication Failures

Crisis communication systems can fail in a variety of ways. To shed light on the many different failures that degrade and undermine such systems, this report identifies four categories of pathways to failure: **operational failures**, **adversarial failures**, **accidental failures** and **institutional failures**. Each category is made up of specific types of failures, investigated in further detail in the following sections of this report.



OPERATIONAL FAILURES



Failures driven by breakdowns in the way in which communication systems are operated, maintained, repaired, and rehearsed

- Physical degradation from standard wear and tear
- Physical failure from lack of maintenance
- Loss of operational readiness and memory
- Insufficient upgrades and modernization
- Lack of TEVV



ADVERSARIAL FAILURES

Failures caused intentionally by adversarial actors interacting with the system



- Intentional severing of communication lines
- Third Party Sabotage
- Cyber attacks and cyber espionage
- Malign information flows reduce trust in the system and messages conveyed through the system
- Electronic Warfare



ACCIDENTAL FAILURES

Incidents of failure driven by unexpected, inadvertent breakdowns in the system



or unexpected, inadvertent events that impact the system



- Physical degradation from environmental events (eg. solar blasts)
- Accidental system failure
- Message is unintentionally not received
- Accidental personnel failure



INSTITUTIONAL FAILURES

Failures driven by behaviors and procedures (or lack thereof)



that inhibit the use of the system

- More convenient alternatives
- Message is intentionally not received
- Lack of trust in the system
- Political dilemmas or lack of procedures in communication

This organizational framework helps to re-evaluate historical nuclear, military, diplomatic, or crisis communication failures, thereby suggesting how such failures can be prevented or mitigated in present day systems. There are also lessons to be learned in how failures have historically been overcome.

Operational Failures

This report defines operational failures as failures driven by breakdowns in the way in which communication systems are used, rehearsed, maintained, and repaired. These failures are the result of operator error or neglect, rather than a lack of procedures and maintenance standards.

Though these failures are often caused by long term action or lack thereof, the failure happens unexpectedly and therefore seems instantaneous. That seeming immediacy of the failure may mislead operators about its cause and maintenance personnel may simply fix the broken or malfunctioning component without examining the systemic cause.





Operational Failures | Failures driven by breakdowns in the way in which communication systems are operated, maintained, repaired, and rehearsed



1.1 PHYSICAL DEGRADATION FROM STANDARD WEAR AND TEAR

Communication infrastructure routinely breaks down or is qualitatively affected when exposed to environmental forces and routine use.



1.2 PHYSICAL FAILURE FROM LACK OF MAINTENANCE

The system experiences loss of reliability, efficiency, or usability due to lack of regular maintenance, ineffective repairs, or poorly monitored (and thus not resolved) problems.



1.3 LACK OF TEVV

Insufficient Testing, Evaluation, Verification, and Validation (TEVV) in peacetime may result in errors and failures in the system going undetected in times of crisis, leading the system to fail at the worst moment.



1.4 PHYSICAL FAILURE FROM LACK OF MAINTENANCE

Insufficient upgrades and modernization may prevent a system from performing reliably and securely. Modernization is also critical for systems to evolve their defenses against evolving, emerging, and accelerating threats.



1.5 LOSS OF OPERATIONAL READINESS AND MEMORY

After change of personnel or lack of use, a system is less (or not) used, due to inadequate knowledge of the system and the procedures of operation.

Historical Operational Failures

Many operational failures are never made public, as they may go unnoticed, be ignored, be covered up out of embarrassment, or be quickly fixed without addressing the systemic causes. Acknowledging operational failures may also require sharing sensitive information about how a system operates. A particularly concerning example of lost operational readiness and memory can be found in the crisis response at NORAD during the September 11, 2001 attacks:

“NORAD (the North American Aerospace Defense Command in Colorado Springs) asked three times for inclusion of an FAA representative (Federal Aviation Administration) in the conference call with the NMCC. NORAD’s first request for this was at 10:03 am Colorado time on 9/11. It was only at 10:17 am that an FAA representative did join the call. But this individual knew nothing about emergency response procedures, either of the FAA or the NMCC. He also had no access or communications to other FAA officials who might have such knowledge.” [Paul Bracken, Communication Disruption Attacks on NC3](#)

Accidental Failures

This report defines accidental failures as **failures driven by unexpected, inadvertent breakdowns in the system, or unexpected, inadvertent events that impact the system.**

These failures can be anticipated broadly, but the specific events are rarely expected and usually necessitate a rapid response. These failures are also specifically non-adversarially derived—the blame for these failures falls either on the environment surrounding the system, the people surrounding the system, or other unexpected instantaneous events.

These instantaneous events can include climate change and extreme weather,¹ solar storms, and other environmental events that can unexpectedly impact communication systems; a physical component of the system failing without obvious cause; and accidental personnel or system use failures, such as personnel inadvertently sending a message improperly or failing to realize that one had been sent. These failures can be either without obvious cause or without expected/long term cause. For example, one could expect extreme weather to disrupt a communication system but a particularly strong storm could seriously damage communication infrastructure and take a system offline for an extended period of time.



1. Fortifying against extreme weather is also a part of mitigating the danger posed to systems by climate change. As climate change accelerates, the world will see increasingly strong storms and inclement weather.



Accidental Failures | Incidents of failure driven by unexpected, inadvertent breakdowns in the system, or unexpected, inadvertent events that impact the system



2.1 PHYSICAL DEGRADATION FROM ENVIRONMENTAL EVENTS (EG. SOLAR BLASTS)

Environmental events can disrupt the reliability and usability of a communication system. These events can be both kinetic (an earthquake taking out receiving towers) and non-kinetic (a solar flare disrupting radio communications).



2.3 MESSAGE IS UNINTENTIONALLY NOT RECEIVED

A leader can try to communicate with another, the system can operate as required, but the receiving leader may be unintentionally, or unknowingly, unable to acknowledge the message or “pick up” the line.



2.2 ACCIDENTAL SYSTEM FAILURE

The system experiences loss of reliability, efficiency, or usability due to lack of regular maintenance, ineffective repairs, or poorly monitored (and thus not resolved) problems.



2.4 ACCIDENTAL PERSONNEL FAILURE

Personnel operating communication systems may inadvertently send the wrong communication, send a communication at the wrong time, or fail to send a communication.

Historical Operational Failures

Since accidental failures are unexpected, they can fail at the best or the worst times. An unknown accidental failure in a time of crisis may be interpreted as the start of an attack. This unhappy coincidence was on display in 1961, a tense year in the Cold War during which the Berlin Crisis occurred, when the communication link between NORAD and the Strategic Air Command Headquarters accidentally failed. The SAC was cut off from three ballistic missile early warning systems and [was left wondering](#) if they were under attack.

Likewise, during the September 11, 2001 attacks the White House experienced significant difficulties in reaching President Bush on Air Force One. These difficulties became dire when President Putin, concerned about the [increased nuclear alert level](#) of American forces, [sought to speak to President Bush](#) and seek reassurances. Since the White House could not reach the American president, President Bush was unable to respond to President Putin.

Adversarial Failures

This report defines adversarial failures as **failures caused intentionally by adversarial actors interacting with the system.**

These failures are intentionally triggered, though some impacts of them can be unanticipated.

There are many ways that adversaries may cause the failures of a system and those adversaries may have several different motivations behind causing those failures. Non-kinetic adversarial failures include hacks of communication systems, cyber espionage, and supply chain attacks. Kinetic attacks include attacks on undersea cables, anti-satellite attacks, EMP and electronic warfare. Adversarial attacks are particularly detrimental to trust in the system, as many states see having a sensitive message intercepted as riskier than having a sensitive message fail to send. While all adversarial failures can erode trust in a system, insider threats, espionage, and cyber threats are particularly corrosive.

Adversarial attacks also do not have to come from external adversaries or competitors. Communication systems risk attacks from insiders, as well as intentional actions taken by anti-government groups and rogue factions in government to sabotage communications systems potentially seeking to block negotiations or progress on objectives they oppose.





Adversarial Failures | Failures caused intentionally by adversarial actors interacting with the system



3.1 INTENTIONAL SEVERING OF COMMUNICATION LINES

In times of conflict or tension, countries may physically sever communications ties. This may be done by exploding communication infrastructure, physically disconnecting the network, or ceasing to staff and operate the communication system.



3.2 THIRD PARTY SABOTAGE

Groups, countries, or organizations not party to the communication system may try to sabotage the system in order to impede communications. This might be done through kinetic or non-kinetic action (as discussed in 3.3, 3.4, and 3.5).



3.3 ELECTRONIC WARFARE

Crisis communication systems and hotlines may face intentional jamming or other types of electronic warfare, which is the use of the electromagnetic spectrum and directed energy to disable adversary assets.



3.4 CYBER ATTACKS AND CYBER ESPIONAGE

Groups, countries, or organizations not party to the communication system may attempt to disable it through cyber attacks, or may attempt to infiltrate intelligence gathering operations with cyber espionage. This category includes supply chain attacks, as well as collateral damage from more general exploits against military or civilian communications.



3.5 MALIGN INFORMATION FLOWS REDUCE TRUST IN THE SYSTEM AND MESSAGES CONVEYED THROUGH THE SYSTEM

Disinformation narratives, imposters spreading false messages, and communication siloes limiting important information from getting through to officials and decision-makers may reduce trust in the system, the counterpart at the other end of the system, and messages conveyed through the system.

Historical Operational Failures

There is a long history of adversarial attacks on communication systems. At the outset of most conflicts communication systems are a priority target, often with the aim of weakening an adversary's advance or defense. With military communication systems one of the first targets at the onset of conflict, crisis communications risk being taken out as collateral, if not potentially outrightly targeted themselves.

These attacks can include cyber attacks, which are top of mind given the DDoS attacks and satellite hacks that Russia inflicted on Ukraine during the early stages of the Russo-Ukrainian War. Beyond the non-kinetic, there can be the plain and simple blowing up of communication systems, as the Chetniks did in the Second World War and North Korean Dictator Kim Jong Un directed in the 2020 destruction of the Inter Korean Liaison office.

Not only do crisis communication systems risk destruction in war, but during conflicts, in their lead up, and even in peacetime, there are attractive incentives for states to infiltrate communication systems for espionage or to plant ideas. In recent years, several world leaders have been targeted by prank callers who manage to talk their way into conversations with world leaders. More recently, the Pegasus spyware exploit infiltrated the personal communication devices of [several world leaders](#), including French President Emmanuel Macron and then Pakistani Prime Minister Imran Khan.

Institutional Failures

This report defines institutional failures as **failures driven by systemic behaviors and procedures (or lack thereof) that inhibit the use of the system.**

These failures range from governments and national leaders being unwilling to use the system, to domestic factions and political disagreements impeding the use of the system, to the separation of communication operators—physically or bureaucratically—from those who make the decision to use the communication system. This category also includes failures to “pick up the phone,” the absence of institutional protocols and mechanisms, and leaders’ use of commercially available communication technology to communicate with their counterparts or their populations.





Institutional Failures | Failures driven by behaviors and procedures (or lack thereof) that inhibit the use of the system



4.1 MORE CONVENIENT ALTERNATIVES

Officials may be drawn to communicating through other, less secure, less resilient, and less formal channels, and as such, neglect use of hotlines and crisis communications.



4.2 MESSAGE IS INTENTIONALLY NOT RECEIVED

Even after a leader attempts to communicate with another leader and successfully operates the system the receiving leader may not want to acknowledge the message or “pick up” the line.



4.3 LACK OF TRUST IN THE SYSTEM

A system may not be used to its full potential due to a lack of trust. The fears underpinning this lack of trust could include:

1. Fears of impersonation (point of failure 3.4);
2. Fear of accepting foreign hardware and software;
3. Fears of further sharing of the information given to counterparts



4.4 POLITICAL DILEMMAS OR LACK OF PROCEDURES IN COMMUNICATION

Communication systems may not be used if governments fail to have the proper procedures in place to notify those with authority to make the call, or if those with authority to make the call fear the political repercussions of communicating with an adversary.

Historical Operational Failures






Perhaps the most pertinent institutional failure is the present, ongoing difficulty that American officials say they face in reaching Chinese counterparts. Though the U.S. has a hotline with China, numerous American officials have said that the Chinese government is not interested in “picking up.” [In a recent IST event](#), panelist Dr. Tong Zhao noted that this reluctance to use crisis communication channels stems from a Chinese fear that those channels may be used by adversaries and competitors to spread disinformation.

A particular institutional concern is leaders’ dependence on personal communication devices and commercial communication systems. French President Macron uses WhatsApp to communicate with members of his government and international counterparts. While that approach is certainly convenient, concerns that his [messages had been targeted](#) by Pegasus Spyware and compromised forced him to change phones. Personal, insecure phones of leaders and decision-makers have also been [targeted by prank callers](#) pretending to be other international world leaders and decision makers.

Patching Points of Failure

Within the framework of operational, adversarial, accidental, and institutional points of failure in crisis communications, some failures are easier to mitigate than others. These failures might be simpler to mitigate technically, may be mitigated unilaterally (reducing the need for grueling negotiations), or may simply require new protocols. While all crisis communication points of failure should be of concern to the leadership of states with nuclear weapons, there are some points of failure that can be tackled more easily, which might demonstrate a viable pathway for future mitigation and build appetite for more failure prevention efforts.

Of the points of failure discussed in this report, the operational and institutional failures categories offer the most hope for feasible mitigation. The following five points of failure suggest quick wins:

	OPERATIONAL FAILURES	Physical failure from lack of maintenance
	OPERATIONAL FAILURES	Loss of operational readiness and memory
	OPERATIONAL FAILURES	Insufficient upgrades and modernization
	INSTITUTIONAL FAILURES	More convenient alternative communication systems
	INSTITUTIONAL FAILURES	Political dilemmas or lack of procedures in communication

These points of failure make for good starting points in mitigation. Not only are these failures easier to resolve, they may be less sensitive to disclosure relative to mitigations like increased cybersecurity mechanisms. The above five points of failure can be mitigated through updating protocols, regular maintenance, and rehearsal, as follows:

Physical failure from lack of maintenance: Improved and more intentional regular maintenance of systems. Though crisis communications may only be used at certain unexpected moments, their maintenance should be ongoing.

Loss of operational readiness and memory: Regular use of systems, with regular internal rehearsals, and regular practice runs with counterparts. Additionally, efforts should be made to increase the pool of personnel who can operate the systems, so that in the event of staff shortages or unavailability, there is always sufficient personnel to send a message.

Insufficient upgrades and modernization: Regular upgrades and modernization, particularly with an eye towards 1) keeping the system protected from disruptive emerging technologies and 2) keeping the system usable and efficient as a communication device vis-à-vis modern communication technologies.

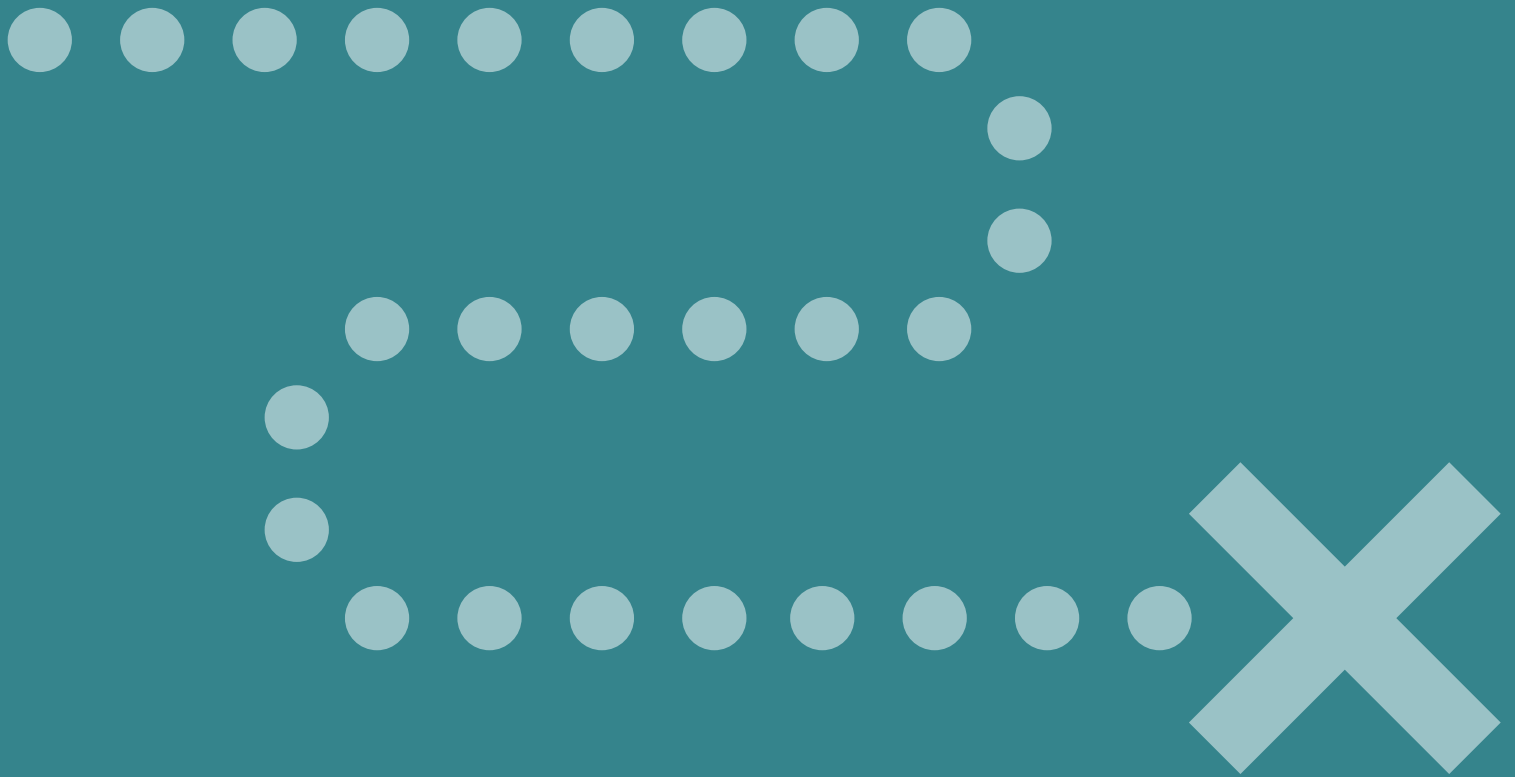
More convenient alternatives: Continued development of communication devices that can compete with the usability and efficiency of the modern day devices. Relatedly, leaders and government employees should be continuously reminded of the threats and vulnerabilities associated with using commercial communication technologies for diplomatic purposes.

Political dilemmas or lack of procedures in communication: Developing (and adhering to) clear procedures, delegations, and conditions for use. Should an incident occur, there should be a clear understanding throughout the chain of command on whether the incident warrants communication, who makes the decision to communicate, who determines the message contents, and who sends the message. Decision-makers should know whether they are authorized to send messages and to whom they are authorized to delegate authority.

Conclusion

The current strategic environment, though tense and occasionally hostile, is not a death sentence for crisis communications. Rather, it could be exactly the impetus needed for a renewed commitment to communicating as a means of reducing nuclear risks. The first great era of reducing nuclear risks through effective crisis communications came during the Cold War, after the two superpowers nearly destroyed the Earth in a nuclear exchange. The successful efforts to increase nuclear crisis communications after the Cuban Missile Crisis should be taken as inspiration to reinvigorate crisis communication. In the 21st century, strengthening crisis communications in the face of strategic competition, waning arms control, new disruptive technologies, and reduced decision-making time constraints would enable states to sustain strategic stability.

Appendix 1: Points of Failure in Nuclear Crisis Communications



Operational Failures



Failures driven by breakdowns in the way in which communication systems are operated, maintained, repaired, and rehearsed



1.1 PHYSICAL DEGRADATION FROM STANDARD WEAR AND TEAR

Communication infrastructure routinely breaks down or is qualitatively affected when exposed to environmental forces and routine use.

EXAMPLE

*"The military-operated India-Pakistan hotline established after the 1971 war was seen for decades as "noisy and unreliable with frequent breakdowns.""*¹



1.2 PHYSICAL FAILURE FROM LACK OF MAINTENANCE

The system experiences loss of reliability, efficiency, or usability due to lack of regular maintenance, ineffective repairs, or poorly monitored (and thus not resolved) problems.

EXAMPLE

*A study found that "Human errors account for most failures in major weapons and space vehicles, more so than mechanical or technical failure." This is a major point of concern if applied to nuclear crisis communications.*²



1.3 LACK OF TEVV

Insufficient Testing, Evaluation, Verification, and Validation (TEVV) in peacetime may result in errors and failures in the system going undetected in times of crisis, leading the system to fail at the worst moment.

EXAMPLE

*As a positive example of TEVV, the U.S. and Russia maintain regular tests of the MOLINK DC-Moscow hotline to ensure its ability to function properly.*³



1.4 INSUFFICIENT UPGRADES AND MODERNIZATION

Insufficient upgrades and modernization may prevent a system from performing reliably and securely. Modernization is also critical for systems to evolve their defenses against evolving, emerging, and accelerating threats.

EXAMPLE

*"The military-operated India-Pakistan hotline established after the 1971 War was seen for decades as "noisy and unreliable with frequent breakdowns.""*⁴



1.5 LOSS OF OPERATIONAL READINESS AND MEMORY

After change of personnel or lack of use, a system is less (or not) used, due to inadequate knowledge of the system and the procedures of operation.

EXAMPLE

*During the September 11, 2001 terrorist attacks, NORAD requested that a FAA representative joining a conference call with the National Military Command Center. NORAD had to request a representative three times and wait 15 minutes before a FAA representative joined the call. However, "this representative knew nothing about emergency response procedures, either of the FAA or the NMCC. He also had no access or communications to other FAA officials who might have such knowledge."*⁵

Accidental Failures



Incidents of failure driven by unexpected, inadvertent breakdowns in the system, or unexpected, inadvertent events that impact the system



2.1 PHYSICAL DEGRADATION FROM ENVIRONMENTAL EVENTS (EG. SOLAR BLASTS)

Environmental events can disrupt the reliability and usability of a communication system. These events can be both kinetic (an earthquake taking out receiving towers) and non-kinetic (a solar flare disrupting radio communications).

EXAMPLE

"Geomagnetic storms can impact infrastructure in near-Earth orbit and on the surface, potentially disrupting communications, the electric power grid, navigation, radio, and satellite operations."⁶



2.2 ACCIDENTAL SYSTEM FAILURE

A physical component of the system accidentally fails, reducing the reliability, efficiency, or usability of the system.

EXAMPLE

In 1961, communications link between NORAD and the Strategic Air Command Headquarters accidentally failed, cutting the Strategic Air Command off from three Ballistic Missile Early Warning systems and leaving the Strategic Air Command wondering if they were under attack.⁷



2.3 MESSAGE IS UNINTENTIONALLY NOT RECEIVED

A leader can try to communicate with another, the system can operate as required, but the receiving leader may be unintentionally, or unknowingly, unable to acknowledge the message or "pick up" the line.

EXAMPLE

During the September 11, 2001 terrorist attacks, Russian President Vladimir Putin attempted to reach American President George W. Bush but the White House was unable to reach President Bush and connect the two.⁸



2.4 ACCIDENTAL PERSONNEL FAILURE

Personnel operating communication systems may inadvertently send the wrong communication, send a communication at the wrong time, or fail to send a communication.

EXAMPLE

In 2018 an emergency alert was sent out in Hawaii by human error, falsely warning that a ballistic missile attack was imminent.⁹

Intentional/Adversarial Failures



Failures caused intentionally by adversarial actors interacting with the system



3.1 INTENTIONAL SEVERING OF COMMUNICATION LINES

In times of conflict or tension, countries may physically sever communications ties. This may be done by exploding communication infrastructure, physically disconnecting the network, or ceasing to staff and operate the communication system.

EXAMPLE

In 2020, the North Korea destroyed its joint liaison office with South Korea as part of an effort to sever communication ties.¹⁰



3.2 THIRD PARTY SABOTAGE

Groups, countries, or organizations not party to the communication system may try to sabotage the system in order to impede communications. This might be done through kinetic or non-kinetic action (as discussed in 3.3, 3.4, and 3.5).

EXAMPLE

During the Second World War, the Yugoslav Army conducted sabotage of Axis communication lines, with help and encouragement from the United Kingdom.¹¹



3.3 ELECTRONIC WARFARE

Crisis communication systems and hotlines may face intentional jamming or other types of electronic warfare, which is the use of the electromagnetic spectrum and directed energy to disable adversary assets.

EXAMPLE

Russia jammed signals from global positioning systems (GPS) satellites in Ukraine at the onset of the Russo-Ukrainian War.¹²



3.4 CYBER ATTACKS AND CYBER ESPIONAGE

Groups, countries, or organizations not party to the communication system may attempt to disable it through cyber attacks, or may attempt to infiltrate intelligence gathering operations with cyber espionage. This category includes supply chain attacks, as well as collateral damage from more general exploits against military or civilian communications.

EXAMPLE

The Russian military hacked a Ukrainian military communication satellite in the early days of the Russo-Ukrainian War.¹³



3.5 MALIGN INFORMATION FLOWS REDUCE TRUST IN THE SYSTEM AND MESSAGES CONVEYED THROUGH THE SYSTEM

Disinformation narratives, imposters spreading false messages, and communication siloes limiting important information from getting through to officials and decision-makers may reduce trust in the system, the counterpart at the other end of the system, and messages conveyed through the system.

EXAMPLE

Russian prank callers Volvan and Lexus have successfully managed to speak to a number of world leaders, including Boris Johnson, Kamala Harris and Emmanuel Macron by pretending to be other world leaders.¹⁴

Institutional Failures



Failures driven by behaviors and procedures (or lack thereof) that inhibit the use of the system



4.1 MORE CONVENIENT ALTERNATIVES

Officials may be drawn to communicating through other, less secure, less resilient, and less formal channels, and as such, neglect use of hotlines and crisis communications.

EXAMPLE

Many leaders and diplomats, including French President Emmanuel Macron, are drawn to using messaging apps including WhatsApp and Telegram to communicate with each other. Following reports that he was targeted by Pegasus Spyware, President Macron was forced to change phones after concerns that his messages had been compromised.¹⁵



4.3 LACK OF TRUST IN THE SYSTEM

A system may not be used to its full potential due to a lack of trust. The fears underpinning this lack of trust could include:

1. Fears of impersonation (point of failure 3.4);
2. Fear of accepting foreign hardware and software;
3. Fears of further sharing of the information given to counterparts

EXAMPLE

"The military-operated India-pakistan hotline established after the 1971 war was seen for decades as "noisy and unreliable with frequent breakdowns."¹⁷



4.2 MESSAGE IS INTENTIONALLY NOT RECEIVED

Even after a leader attempts to communicate with another leader and successfully operates the system the receiving leader may not want to acknowledge the message or "pick up" the line.

EXAMPLE

Chinese officials often do not "pick up the phone" when called by their U.S. counterparts, or refuse to be available for those calls in the first place.¹⁶



4.4 POLITICAL DILEMMAS OR LACK OF PROCEDURES IN COMMUNICATION

Communication systems may not be used if governments fail to have the proper procedures in place to notify those with authority to make the call, or if those with authority to make the call fear the political repercussions of communicating with an adversary.

EXAMPLE

As Steven Miller notes in "intended for use at the highest levels of government, the US-Russia Hotline, by design, short-circuits the normal policy process and can at least temporarily exclude most of the government and the military from information flows." Those excluded from the communication may react poorly, in a way that disincentivizes communication that does not involve broader consultations.¹⁸

Endnotes



- 1 <https://foreignpolicy.com/2021/04/19/zoom-hotline-red-telephone-nuclear-war-cuban-missile-crisis/>
- 2 <https://www.ncbi.nlm.nih.gov/books/NBK219146/>; <https://time.com/44648/u-s-faces-challenges-maintaining-aging-nuclear-arsenal/>
- 3 https://securityandtechnology.org/wp-content/uploads/2020/07/bracken_comm_disruption_IST-1.pdf
- 4 <https://southasianvoices.org/hotline-between-command-authorities-to-manage-tensions/>
- 5 <https://2009-2017.state.gov/t/isn/4785.htm>
- 6 <https://breakingdefense.com/2022/08/noaa-warns-strong-solar-storm-possible-could-disrupt-gps-radio-communications/>
- 7 <https://futureoflife.org/resource/nuclear-close-calls-a-timeline/>
- 8 <https://www.nbcnews.com/storyline/9-11-anniversary/secrets-9-11-new-details-chaos-nukes-emerge-n645711>
- 9 <https://www.nytimes.com/2018/01/13/us/hawaii-missile.html>
- 10 <https://www.npr.org/2020/06/16/877887300/in-terrific-explosion-north-korea-blows-up-liaison-office>
- 11 https://www.cia.gov/readingroom/docs/OSS%20-%20SSU%20-%20CIG%20EARLY%20CIA%20DOCUMENTS%20%20%20VOL.%205_0015.pdf
- 12 <https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say/>
- 13 <https://securityandtechnology.org/wp-content/uploads/2022/07/Playing-Telephone-Hoax-Calls-and-the-Insecurity-of-Leader-to-Leader-Communications.pdf>
- 14 <https://www.space.com/russia-jamming-gps-signals-ukraine>
- 15 <https://www.bbc.com/news/world-europe-57937867>
- 16 <https://www.politico.com/news/2021/09/01/us-china-military-hotline-508140>
- 17 <https://securityandtechnology.org/wp-content/uploads/2022/07/Playing-Telephone-Hoax-Calls-and-the-Insecurity-of-Leader-to-Leader-Communications.pdf>
- 18 <https://securityandtechnology.org/wp-content/uploads/2020/10/Hotlines-Origins-Evolution-Application-StevenMiller.pdf>

