2018 IEEE International Conference on Software Quality, Reliability and Security Companion

Space-based Unidirectional Networks and Resiliency

Vaughn H. Standley
College of Information and Cyberspace
National Defense University
Washington D.C., U.S.A.
vaughn.standley.civ@ndu.edu

Edward A. Boucheron
Civil Systems Group
The Aerospace Corporation
Albuquerque, NM U.S.A
edward.a.boucheron@aero.org

***Abstract* — The bidirectionality of networks makes them resilient, but also vulnerable to propagating failures from cyber-attacks. Unidirectional systems are mostly immune to cyber-attack. The radio navigation component of the Global Positioning System (GPS) is unidirectional. However, it may be assessed as a bidirectional network when it is used to provide equivalent information in place of terrestrial networks that have failed. GPS thus serves as a case study for a novel mathematical formulation of the contribution of space-based unidirectional systems to the resilience of strategic cyber networks. The technical basis for this formulation is a parametric model of the exceedance probability for N GPS satellites in view of a receiver. The exceedance probabilities form an N+1 node network whose spectral radius can be computed. Three resiliency attributes for space-based unidirectional networks that use the resulting spectral radii are examined: connectedness as a function of failure, unidirectionality, and directness.**

Keywords—GPS; Cybersecurity; Resiliency; Unidirectional; Network

I. INTRODUCTION

Nations are increasingly seeking strategic-level cyber networks that are survivable and resilient. Resiliency is described qualitatively as the ability to resist, absorb, recover from, or successfully adapt to adversity or change in conditions [1]. While the Internet is vast and resilient by design, it is not controlled by any one nation and has become famously vulnerable to hacking and transmitting misinformation. In some cases, space-based systems are the only economic means to provide network connectivity, with satellite based radio systems survivable by design and less accessible to cyber tampering than land-based systems.

There are three main satellite orbits used for communications: geosynchronous (GEO), medium earth orbit (MEO), and low earth orbit (LEO). Satellites in the GEO orbit persist over the same point on the earth, but at 30,000 km distance from the earth's surface require high transmission power or large dish receivers compared to lower altitude orbits. MEO is the home of most navigation satellites because it maximizes global coverage with a minimum number of satellites. Systems in LEO are closer to the Earth's surface, so the required transmission power is less, but maintaining persistent coverage becomes the issue due to the limited line of sight from a LEO satellite to the earth surface. For example, 86 Iridium satellites in LEO are needed to ensure global coverage, where GPS satellites operating in MEO only needs 24. Improvements in satellite technology and the emergence of commercial launch capability are making satellite information systems increasingly attractive for each of these orbits. The radio navigation component of GPS is unidirectional. However, it may be assessed as a bidirectional network when it is used to provide equivalent information in place of terrestrial networks that have failed. GPS thus serves as a case study for a novel mathematical formulation of the contribution of space-based unidirectional systems to the resilience of strategic cyber networks.

II. CASCADING NETWORK FAILURE & RESLIENCY

A measure of resilience may be obtained through the exceedance probability used in traditional quantitative risk management. Unpredictable and catastrophic failures in networked systems are often observed to follow a power law relationship, meaning that the probability of a consequence value of c occurring that exceeds a consequence level C is equal to c raised to a negative constant q:

$$P(c > C) = c^{-q} \quad (1)$$

Intuitively, the power law means that smaller consequence events happen exponentially more often than larger events. Systems that follow a power law are identified as "low risk" if $q > 1$ because the probabilities of extremely high consequence events are vanishingly small. Conversely, they are "high risk" if $q < 1$. Figure 1 illustrates the applicability of the power law to electric power distribution system outages. It plots the exceedance probability of outages with greater than a load loss of level L. For $L > 500$ MW, the log-log relationship between exceedance probability and L is linear and the slope is $-q$. The value q is the fractal dimension of this exceedance relationship.

Failures start and propagate in a network according to the vulnerability probability of nodes, γ, and the network spectral radius, ρ. Spectral radius embodies the main characteristics of a bidirectional network, which are the density of links and size of heavily connected hubs. The measure of network resilience, z, is proportional to the inherent fractal dimension of the network, q, and is also proportional to $\gamma\rho$, where $z < 1$ indicates low risk, $z > 1$ is high risk, and $z >> 1$ indicates the potential for catastrophe. Spectral radius can be seen as a measure of "reachability" from any one node to any other node along a

978-1-5386-7839-8/18/$31.00 ©2018 IEEE
DOI 10.1109/QRS.2018.00058

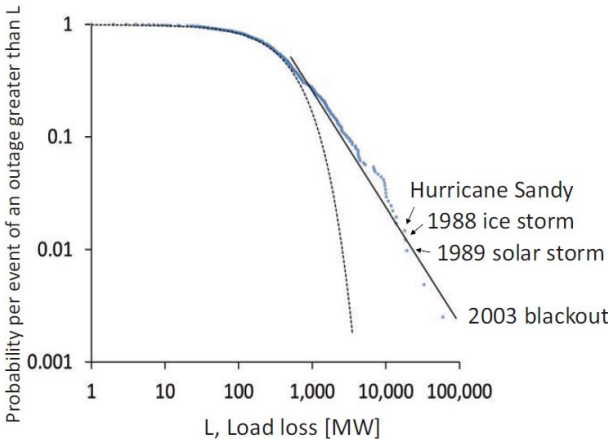

Figure 1: Dots indicate actual outage events. The dashed line is a exponential distribution fit to the failures below 500 MW. The solid line is a power law fit for failures above 500 MW [2].

chain of network hops. As reachability increases, vulnerability to cascading failure increases. The product $\gamma\rho$ will determine the degree to which failures propagate. The logarithm of q varies in a linear fashion with respect to $\gamma\rho$, where b and k are y-axis offset and proportionality constants, respectively [3]:

$$log(q) = b + k\gamma\rho \quad (2)$$

In this formulation, the left-hand-side is positive for low-risk systems and negative for high-risk systems and b can be interpreted to be the margin between high and low risk behavior. The second term on the right hand side, $k\gamma\rho$, represents the loss to this margin due to propagating failures in the network (where k is negative). Survivability of a network can be achieved by hardening nodes or isolating them from the network as soon as the node has been compromised. For example, in a network model for the communicability of a human disease, nodes in the network represent humans who may receive preventive treatment to reduce infectiousness, decreasing γ. Or, links in the network are cut by enforcing a quarantine to reduce ρ. Unidirectional communication systems do not have a $k\gamma\rho$ term because failures or computer viruses cannot travel upstream to the broadcasting node.

A novel approach to analyzing these systems is to treat the unidirectional broadcast network as effectively bidirectional by crediting the informational value of the message and recognizing that the system is invulnerable to cyber threats due to its unidirectional property. The capability that is not lost for this case can be estimated by computing the $k\gamma\rho$ term using the spectral radius of the unidirectional network. The issue that arises with this approach is computing a meaningful value of the spectral radius ρ, the largest non-zero eigenvalue of the network's connection matrix, given that unidirectional connection matrices result only in eigenvalues of zero. To assess the resiliency of networks that contain or are backed-up by unidirectional systems, it is necessary to extend the abstraction of unidirectional information in terms of the network connection matrix.

III. The Bidirectionality of Some Broadcast Networks

Unidirectional networks allow data to travel only in one direction to guarantee information security. They are commonly found in high security environments where they serve as an information diode between two or more networks of differing security classifications. From an information theory perspective, unidirectional transmission systems can convey as much information as a bidirectional system [4]. An analysis of the bidirectionality of these systems is motivated by the evolving threat to normal bidirectional networks and the common sense belief that broadcasted information must be able to contain information value that can compensate for these networks during operation or when they are compromised.

Strictly speaking, bidirectional networks are pairs of unidirectional channels that transmit and receive in opposite direction. The Internet is an example of an electronic network that built on these pairs to enable instant human-to-human two-way communications as well as server-based applications that respond to individual human or software robot queries. From the standpoint of a user of the system the only difference between one-way and two-way communication is the quantity of information directly relevant to a question posed by the user versus the amount of random transmission that is not of interest. Unidirectional networks contain the equivalent of bidirectional information if they are designed to continuously answer a specific question – the question being in one direction, the answer in the other. The "two-way-ness" of broadcast information thus takes credit for the specific question they are designed to answer. In this version of a "Turing Test" [5], a unidirectional system is a bidirectional system to the extent that it behaves like one—the observer cannot discern whether the system is unidirectional or bidirectional based on its behavior. To give a sense of this, consider the following questions and answers normally considered two-way communication:

A. *Clock*

Q: What is the time? A: (time)

These days, a growing number of Amazon Alexa owners will ask, "Alexa, what time is it?" In this case, the question is sent to a server via the Internet and the answer returned, "The time is (time)." From an information perspective, however, looking up at a wall clock to answer this question is the same, except that the questioner is simply taking advantage of the continuous information broadcast nature of the clock.

B. *FM Radio Broadcasts*

Q: What's happening locally? A: (Local broadcast news)

Despite being unidirectional, broadcast radio and television seek to provide content perceived to speak directly to each listener to the maximum extent possible, and the shorter the range of the broadcast message, the greater fraction of the content that will apply directly to the listener. However, most of the content will not be directly answering a question posed by the recipient.

C. *The Global Positioning System (GPS)*

Q: Where am I now? A: (x, y, z, t)

From an information perspective, GPS behaves like server that is responding to a very specific question, even though it is completely unidirectional. This realization then becomes the basis for computing the spectral radius of a unidirectional system based on its effective bidirectional connection matrix.

IV. Broadcast GPS RF as a Bidirectional Network

GPS is a resilient-by-design space-based information system. It possess cyber and physical dimensions that are interconnected via networks that form systems of systems. For this reason, GPS is an ideal case study emphasizing a system or process perspective for unidirectional/bidirectional network assessment.

Precise time and satellite location, the main products of GPS, are sent via L-band radio transmissions directly to handheld receivers where they are transformed into real time navigation information. It is not necessary to route the data through potentially compromised online networks. As argued above, GPS behaves like an internet server, but to obtain useful navigation information from GPS, a user must receive signals from at least four satellites. A Kalman filter [6] is a process that runs in embedded software inside handheld GPS receivers, such as modern cell phones, producing increasingly accurate geo-location as it receives telemetry from greater than four satellites. To study this quantitatively, the number of GPS satellites in view of a user is approximated to within 10% by a random distribution based on the geometry depicted in Figure 2 and employing the following mathematical relationship [7]:

$$AverageSatellites\ in\ View = \frac{N_{Total}}{2}\left(1 - sin\left(cos^{-1}\left(\frac{r_e}{r_{sat}}sin(MLA)\right) + (MLA)\right)\right) \quad (3)$$

Figure 3 shows the hypergeometric distribution probabilities for an N_{Total}= 24 satellite GPS constellation (r_{sat} = 20,180 km, r_e= 6,371 km) modeled with an effective 85-degree maximum look-angle (MLA). Selection of 85-degrees is specific to the near straight-line propagation of RF transmissions, where 90-degrees would be the theoretic maximum. Five degrees fewer than 90 takes into account terrain effects and obviates the need to be concerned about any number of satellites greater than 12. The probability density function, P(x=N), shows that the peak number of satellites in view is 8. The exceedance probability (i.e. one minus the cumulative probability) function returns the likelihood that there will be more than N satellites, or P(x>N). From a node and segment perspective, this unidirectional network may be represented as in Figure 4. The geo-location precision for each node is different because it is associated with a different minimum number of satellites in view. For example, the precision for the N > 10 node is greater than for the N > 3 node because the Kalman filter produces higher precision for the greater number of satellites. Thus the spectral radius is abstracted directly to the quality of the data nodes as well as

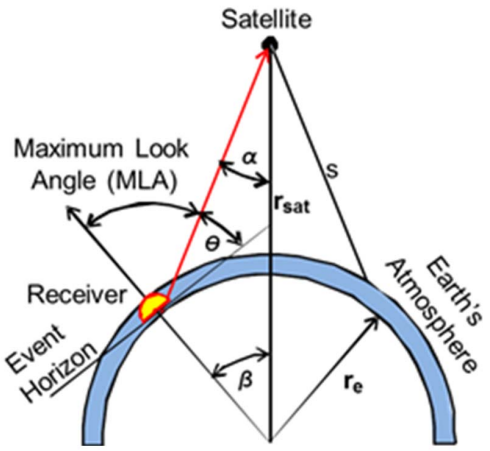

Figure 2: GPS transmission geometry.

the probability that the node will be connected to Node 0, the user. Note that P = 0 for all N > 11 segments and is undefined for N<4.

With this probabilistic model of GPS, the spectral radius of an equivalent two-way network can be estimated by inserting the cumulative probabilities into the top row and first column of a 9-by-9 connection matrix. The result is an eigenvalue matrix for GPS network modelled as a bidirectional network. See Figure 5. The entries represent the strength of the connection between the nodes specified by the column and the row, where the upper row and left column are associated with node 0, the user. In simple connection matrices, entries of 1 or 0 are used, where 1 indicates a guaranteed connection, and 0 means no connection. The strength of the segment connecting node 3 of the satellite to

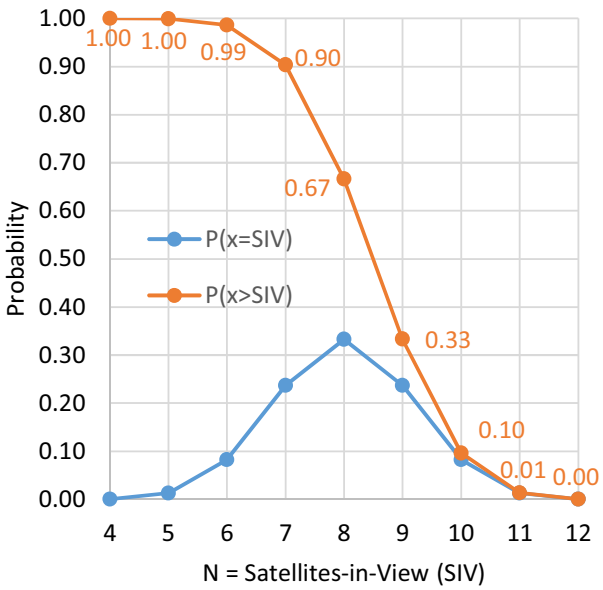

Figure 3: Probability of N satellites in view.

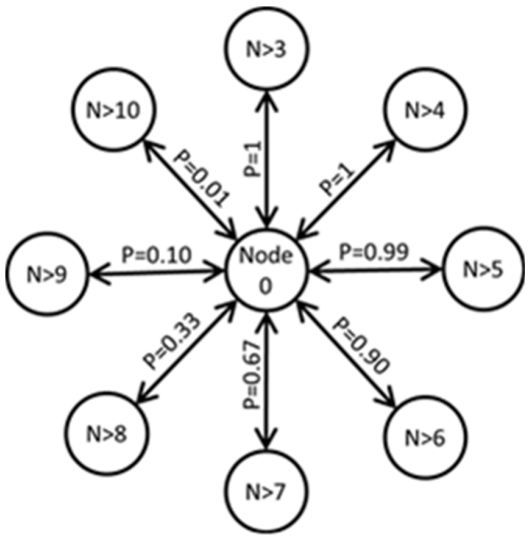

Figure 4: Node and segment diagram of unidirectional GPS Network where N is the number of satellites in view.

the user is, for example, 0.99 or 99/100. All but the first row and left column are zero, meaning there is no communication between these nodes, and nodes do not communicate with themselves.

The spectral radius is the largest nonnegative eigenvalue of the matrix, in this case $\sqrt{43481}/100 = 2.09$. A result greater than one indicates more than four satellites comprise the GPS network. Thus, while GPS might be conventionally viewed as a one-way system with an eigenvalue of zero, it behaves as a significant network and this spectral radius applies to each person operating a GPS receiver in view of the broadcasts.

V. The GPS Unidirectional Network and Resiliency

Resiliency attributes immediately follow from the GPS case study. Three are discussed here as well as how they should be applied.

$$\begin{vmatrix} 0-\lambda & 1 & 1 & \frac{99}{100} & \frac{9}{10} & \frac{67}{100} & \frac{33}{100} & \frac{1}{10} & \frac{1}{100} \\ 1 & 0-\lambda & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0-\lambda & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{99}{100} & 0 & 0 & 0-\lambda & 0 & 0 & 0 & 0 & 0 \\ \frac{9}{10} & 0 & 0 & 0 & 0-\lambda & 0 & 0 & 0 & 0 \\ \frac{67}{100} & 0 & 0 & 0 & 0 & 0-\lambda & 0 & 0 & 0 \\ \frac{3}{10} & 0 & 0 & 0 & 0 & 0 & 0-\lambda & 0 & 0 \\ \frac{1}{10} & 0 & 0 & 0 & 0 & 0 & 0 & 0-\lambda & 0 \\ \frac{1}{100} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0-\lambda \end{vmatrix}$$

Figure 5: GPS Bidirectional Network Eigenvalue Matrix (See https://matrixcalc.org/en/vectors.html)

A. Network Connectedness as a Function of System Failure

Space-based networks help ensure minimum capability remains operational through man-made or natural disasters. But what is the assessed resiliency of the space-based systems themselves in terms of a bidirectional network? The worse-case scenario for GPS information is errors that originate in satellites. Failures in satellites will directly impact all GPS users. For example, if one satellite fails or is disabled, the spectral radius would be reduced to 1.96. This is found by solving (3) using N=11 instead of 12 and solving for the eigenvalues using the resulting exceedance probabilities. Figure 6 demonstrates the graceful degradation of the bidirectional network value of GPS as satellites are removed from the constellation. Greater than six GPS satellites must fail before the resiliency falls below one. Spectral radius values lower than one indicate that fewer than four satellites are in view per the model depicted in Figure 4.

B. Network Unidirectionality

Given the immunity of a unidirectional network to cascading failures, one way to score the ability of a network to resist these failures is to determine the fraction of the network's spectral radius that is unidirectional. This can be computed with a simple ratio:

$$f = \rho_{Unidirectional} / (\rho_{Unidirectional} + \rho_{Bidirectional}) \quad (4)$$

GPS will keep transmitting precise time and location information to unobstructed receivers during a failure of geolocation capability based on cell towers. Bidirectional transmissions from three towers are used by a triangulation algorithm to determine location. A 4-by-4 connection matrix with a spectral radius of $\sqrt{3}$ = 1.79 describes this network, so that f = 2.09 / (2.09 + 1.73) = 0.55. That is, more than half of the U.S. geolocation capability is immune to cascading failure. Note that the cell tower connection matrix can be modeled with 1's and 0's because in the U.S. there are many more towers than are needed for triangulation - it need not be modeled probabilistically as was the case with analyzing GPS location.

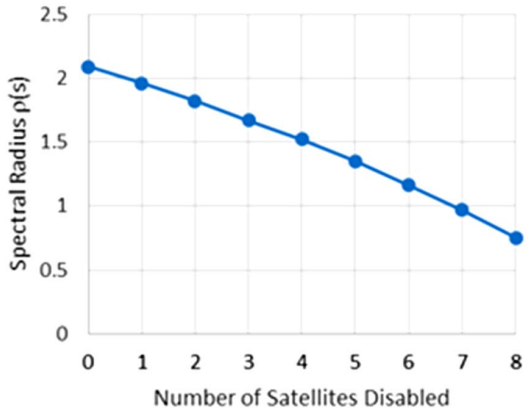

Figure 6: *Spectral radius of GPS unidirectional navigation network as a function of failed satellites*

C. Network Directness

Internet protocol breaks messages down into packets that individually travel to their destination, often through different routes and numerous stops. Packetizing is ideal for public, non-emergency communication because it allows many users to maximally share a limited number of communications channels that have available bandwidth. Unfortunately, maximal use of a system contributes to its susceptibility to cascade failure. With the addition of Public Key Infrastructure, internet messaging can be made relatively secure. However, the ability to intervene or corrupt internet communication exists and is growing. The circuitousness of the path thus adds opportunities to corrupt the validity and trustworthiness of the communication, particularly when the system is under duress. Conversely, the directness of a message is a good measure of the data's security.

Directness is maximized when the network allows communication to travel through the fewest number of segments. Thus, directness is at odds with one of the main features of the Internet (i.e. access to any node in the system). Conversely, one hub with numerous clients, like the GPS network model, maximizes directness. For regular network connection matrixes with 1's and 0's, a hub network with n nodes has the minimum spectral radius of $\sqrt{n-1}$. A measure of directness will thus be the ratio of the minimum spectral radius to the networks actual spectral radius:

$$d = \sqrt{n-1}/\rho(n) \qquad (5)$$

A connection matrix that is connected in every possible way has a spectral radius equal to $(n-1)$. Thus, the least direct network will have a value of $d = \sqrt{n-1}/(n-1)$. Network directness d is thus a fraction ranging from 1 to 0 for increasing $n \geq 2$. GPS is a hub network, so its directness is one.

D. Application of Unidirectional Resiliency Attributes

The theory of cascading failure embodied by (2) suggests that it is reasonable to expect a proportional decrease in the propagation of cascading failure in a bidirectional network when the use of a unidirectional network reduces the use of the bidirectional network. Use of the bidirectional network would decrease if, for example, it were known that attacks were imminent or underway. Thus, the spectral radius in the resiliency loss term z of (2) is replaced by the product $(1\text{-}f)\rho$. So if the unidirectional fraction f is one, then the entire resiliency loss term in (2) vanishes as expected.

Directness should have a similar effect on the resiliency term. The spectral radius in (2) should proportionately decrease with increasing directness, and a completely direct network will be invulnerable to cascading failure according to $(1\text{-}d)\rho$. Given (5), the spectral radius of direct network (d=1) will always be the minimum spectral radius $\rho = \sqrt{n-1}$. But a completely direct network is not necessarily unidirectional. Systems offering both are maximally resistant to cascading failure. Space-based broadcasting systems have the potential to be both unidirectional and completely direct, such as GPS. Of course, there are other ways to interfere with the operation of these systems. But they are not tied to the network properties of the system.

It's worth noting that access to GPS has not always been the case. GPS was a classified military system until Korean Air flight 007 was shot down in 1983, after it inadvertently strayed into Soviet airspace, after which the Reagan administration authorized a limited public access to GPS data. Later, the Clinton Administration declassified all navigation data. With this unrestricted access, the telecommunications industry has made possible everyday use of the system by reducing the cost, size, and power needs of receivers, resulting in the system now being used directly by billions of users.

VI. The Broader Significance of the GPS Case Study

The mathematical formulation developed for the GPS navigation case-study may be applied to numerous other broadcasting systems. Three are briefly considered.

A. Space-based Weather

Extreme weather can claim thousands of lives without proper warning [8]. National Oceanographic and Atmosphere Administration (NOAA) weather satellites in polar orbit provide global coverage twice a day. So while only a fraction of this data will be instantly applicable to the user's location, weather is a complex and relatively slow-moving phenomenon such that conditions measured thousands of kilometers away may directly answer specific questions about future conditions at places of interest. For this reason, satellite-based weather data may be considered to have bidirectional value for assessing network resiliency. Most people get processed weather data rebroadcast by television, radio, or the internet. However, technology advancements have made direct access to satellite weather transmissions as affordable as cell phones. Only a few items (e.g. antenna, software radio) are needed to directly access this data even when the public broadcasting systems have failed. Directly received weather data also avoids the user having to wait for weather broadcast about their specific location, which under some circumstances may be important, such as when power has been lost and users are relying on batteries.

B. The Tsunami Warning Network

Tsunamis are a transcontinental phenomenon where a single event can kill hundreds of thousands of people [9]. The speed of tsunami waves means that the time frame for useful warnings may be only minutes, and at most hours, so it becomes very important to minimize latency-inducing hops. As an example, NOAA issued a tsunami alert 12 minutes after Japan's March 11 2011 earthquake. The tsunami hit the coast of Japan 14 minutes later [10]. Therefore, a continuous, global and rapidly responsive network is needed to issue timely warnings. And while U.S. satellites participate in the collection of instrument data used to detect and estimate the impacts of tsunamis, warnings are not transmitted directly (by satellite or other means). Warnings are prepared and sent out from data collection and processing centers. The recent false alarm experienced in Hawaii of an impending missile attack [11] is a reminder that additional hops are vulnerable to mistakes introduced by human in the loop. The security, timeliness and value of tsunami warnings would be greatly improved if they were issued directly from space.

C. Space-Based Nuclear Detonation Detection

Nuclear weapons have the capability to destroy whole cities, potentially killing millions of citizens. The U.S. Nuclear Detonation Detection System (USNDS) is a space-based system that provides near real-time, worldwide, highly survivable/ endurable capability to detect, locate, and report any nuclear detonations in the earth's atmosphere or near space [12]. It is comprised of many sensors fielded on several different satellite platforms, with many of the instruments being hosted on GPS. The signals produced by a nuclear event are unique, so they can be positively identified as being of nuclear origin. The USNDS system is similar to GPS in that it uses the speed of light and precise time information from at least four satellites to locate nuclear events (that is, in fact, one of the main reasons it has been hosted on GPS satellites). There are many peacetime applications of USNDS data that could greatly benefit the public as well. For example, electromagnetic pulses emitted by lightning strikes are detected by USNDS and can determine the exact position and strength of a thunderstorm, super-cell or eye of a hurricane. Because direct transmissions from USNDS/GPS satellites are all weather and globally available, anyone in or near a large storm would have immediate and unfettered access to this potentially life-saving information. Unlike GPS, however, USNDS data remains classified. Public alerts based on this data would necessarily be distributed by the government.

So long as alert data is not ingested by a bidirectional network, such as the Internet, USNDS will enjoy immunity to cascading failures, as conferred by the nature of unidirectional networks. However, making the warnings public currently would mean that the information must cross over into bidirectional systems, ones that can be compromised, overburdened or rendered inoperative. Declassifying USNDS telemetry would avoid this step and allow direct user access to the broadcasts, increasing the system availability to U.S. military users as well as to other nuclear-armed nations to reduce the likelihood of nuclear false-alarms. [13]

VII. Conclusion

GPS serves as a case study to examine a mathematical formulation of network resilience based on the inherent bidirectional nature of certain broadcast information. The bidirectionality of a unidirectional information system like GPS is based on it being designed to continuously answer a specific *a priori* question, and the straightforward assumption that such broadcast data must in some way compensate for the same information obtained using two-way communication systems. Space-based broadcast systems are immune to cascade failures associated with land-based networks and may help maintain the availability of critical information at critical times, so long as the telemetry is transmitted directly to users. Three attributes appear promising in terms of considering improvements to existing space-based cyber systems to maximize their resiliency: network connectedness as a function of system failure, network unidirectionality, and network directness. More research should be conducted to properly account for the vast potential of unidirectional space-based systems to contribute to resiliency.

Three key public broadcast warning systems were briefly considered in terms of unidirectional resiliency attributes: weather, tsunami, and nuclear attack. These systems highlight the importance of unidirectional space-based broadcasting systems to critical infrastructure but also their unfortunate reliance on bidirectional systems to distribute their content. In the case of the National Weather Service, individual reception of broadcasts has been inhibited by technical complexity and cost and the tradition of incorporating processed weather information in radio and television news. Tsunami warnings are not directly available but warning times could be reduced substantially if data were broadcast directly from satellites. Nuclear detonation information is continuously transmitted to the ground just like GPS telemetry, but is not directly available to the public due to the information still being classified. The resilience of the GPS satellite system and worldwide availability of its broadcasts makes it compelling to wonder if synoptic weather, tsunami, and attack alerts should all be transmitted from the GPS satellite platform.

The opinions, conclusions, and recommendations expressed or implied are the authors' and do not necessarily reflect the views of the Department of Defense or any other agency of the Federal Government, or any other organization.

References

[1] Presidential Policy Directive (PPD) - 21, *Critical Infrastructure Security and Resilience*. February 12, 2013.

[2] National Academies of Science, Engineering, and Medicine. 2017. *Enhancing the Reslience of the Nation's Electrical System*, Washington, D.C.: The National Academies Press. https://doi.org/10.17226/24836.

[3] T.G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, 2e. Wiley, 2015.

[4] C. E. Shannon, "A Mathematical Theory of Communication," *The Bell Systems Journal*, Vol. 27, pp. 379-423, 623-656, July, October, 1948.

[5] A. M. Turing, "Computing Machinery and Intelligence," *Mind*, LIX (236): 433-460, October 1950.

[6] R. E. Kalman, "A New Approach to Linear Filtering and Prediction Problems," *Transactions of the ASME–Journal of Basic Engineering*, 82 (Series D): 35-45, 1960.

[7] V. H. Standley et al., "WIP: Probabilistic Modelling of GPS-based Capabilities," LLNL-CONF-667596, February 23, 2015 [Online] Available: https://e-reports-ext.llnl.gov/pdf/788990.pdf

[8] National Weather Service, "Service Assessment, Hurricane Katrina," U.S. Department of Commerce, National Oceanic and Atmospheric Administration, Silver Spring, Maryland, August 23-31, 2005.

[9] A. Taylor, "Ten Years Since the 2004 Indian Ocean Tsunami," *The Atlantic*, December 26, 2014.

[10] Voice of America, "Tsunami Warning Systems: Lessons from Japan," March 14, 2011. [Online] Available: https://www.voanews.com/a/tsunami-warning-systems-lessons-from-japan-118017249/167190.html.

[11] USA Today Editorial Board, "Hawaii's false alarm should alarm us all," *USA Today*, January 14, 2018.

[12] Defense Technical Information Center, "Exhibit R-2, RDT&E Budget Item Justification, 07 Operational System Development: 0305913F NUDET Detection System (Space)," May 2009. [Online] Avalable: www.dtic.mil/descriptivesum/Y2010/AirForce/0305913F.pdf

[13] V. H. Standley, "What's Missing in the 2018 Nuclear Posture Review," *Real Clear Defense*, March 6, 2018. [Online]. Available: https://www.realcleardefense.com/articles/2018/03/06/whats_missing_in_the_2018_nuclear_posture_review_113153.html.