VOL 1, ISSUE 12 **April 2021**

EDITOR

Dr. Robyn Fiori

IR³ FEATURE ARTICLES

The Infrastructure Resilience Research Group (IR²G), **Office of the Dean, Faculty of Engineering and Design, Carleton University and The Editors of the *"Infrastructure Resilience Risk Reporter (IR³)"* make no representations or warranties whatsoever as to the accuracy, completeness or suitability for any purpose of the Content. Any opinions and views expressed in this online journal are the opinions and views of the authors, and are not the views of or endorsed by *IR²G* or the Office of the Dean. The accuracy of the content should not be relied upon and should be independently verified with primary sources of information. *IR²G* or the Office of the Dean shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to, or arising out of the use of the content.**

The Infrastructure Resilience Risk Reporter (IR³) may occasionally receive unsolicited features and materials, including letters to the editor; we reserve the right to use, reproduce, publish, re-publish, store and archive such submissions, in whole or in part, in any form or medium whatsoever, without compensation of any sort. IR³ is not responsible for unsolicited manuscripts and photographic material.

Editorial Corner

Dr. Robyn Fiori

About the Editor

Dr. Robyn Fiori is a research scientist for the Canadian Hazards Information Service of Natural Resources Canada specializing in space weather. Her research is applied to the development and improvement of space weather tools and forecasts to be used by operators of critical infrastructures and technologies in Canada. Dr. Fiori's research has been published in numerous peer reviewed scientific journals, including the Journal of Geophysical Research, the Journal of Atmospheric and Solar-Terrestrial Physics, and Space Weather. Dr. Fiori received her B.Sc., M.Sc., and Ph.D., from the University of Saskatchewan, Department of Physics and Engineering Physics while studying in the Institute of Space and Atmospheric Studies. She can be reached at robyn.fiori@canada.ca.

This Issue

IR^3 Issue 12 aims to develop an improved understanding of resilience by examining Global Navigation Satellite Systems (GNSS) spoofing, aviation response to space weather alerts, the role of social media in crisis communication, and designs in marine shipping that support green initiatives.

GNSS spoofing attacks are of high relevance to our GNSS-dependent society. **M. Hunter, G. Buesnel, F. Filipi, and D. Martin** attempt to gain insight into the effects of spoofing by carrying out a series of tests on sample GNSS receivers. Such an examination is key for understanding both the impact of spoofing on a GNSS receiver, and the likelihood of an impact to sensitive equipment.

Two articles in IR^3 Issue 9 describe the adoption of a space weather advisory service by the International Civil Aviation Organization (ICAO). **Klaus Sievers and Ralf Parzinger** rightly point out that these advisories are not yet incorporated into the operations manuals of many airlines. In response, they propose procedures to be followed upon reception of these space weather advisories.

The role of social media platforms in crisis communication is discussed by **Xianlin Jin**. Social media represents a publically available 'big data' set that offers potential insight into communication during natural disasters allow organizations to analyze communication flow patterns and develop better strategies for communication. Lessons learned from Hurricane Maria are provided as an example.

Wrapping up Issue 12, **Edward Downing** describes ground-breaking new designs in the shipping industry that bring back the traditional wind-powered approach to marine shipping.

Next Issue

We invite authors to contribute additional articles for Issue 13 relating to their experience in the field of infrastructure resilience. Draft articles of 2500-4000 words are requested by May 14, 2021. You may not have much time or experience in writing 'academic' articles, but IR^3's editorial board can provide guidance and help. Your experience is valuable and IR^3 provides an ideal environment for sharing it.

A Study of the Effects of Spoofing on GNSS Receivers

M. Hunter, G.Buesnel, F.Filipi, D.Martin
Spirent

Abstract

In this paper, the authors carry out an investigation into the effects of GPS spoofing on a small set of sample GNSS receivers.

Our dependence on precise positioning and timing data from space-based positioning systems is very high in key application areas, and as the signals received on Earth from Global Navigation Satellite Systems (GNSS) are of relatively weak power, they are subject to disruption from Radio Frequency Interference (RFI), including spoofing attacks (targeted or incidental). The rise in real-world instances of commercial users suffering significant impacts from spoofing attacks is presented, as is the need to obtain more technical data on the effects of spoofing on user equipment. A simple explanation of the fundamentals of GNSS spoofing is included.

The Authors present a simple static GPS spoofing scenario and present results from a simulation only (all signals including Live Sky and spoofer created in the laboratory). In the discussion of these results, it is clear that a comparison of the impact of Simulation Only spoofing with Authentic Live Sky spoofing (a feed provides GNSS signals from live sky to the receiver where they are combined with the simulator generated spoofing signal) is essential to understanding the likelihood of a spoofing attack compromising user equipment. The test set-up for this extension is shown and a set of results showing the reported ground trajectories of the receivers in Simulated Only and Authentic Live Sky scenarios are shown. The authors discuss the implications of the differences in behaviour across the two test set-ups, present conclusions based on data obtained from both tests, and show the importance of this work in helping to implement test methodologies for emerging Resilient PNT Frameworks. Finally, the authors present some suggestions for follow-up.

I. Introduction

Access to highly accurate positioning, navigation and timing (PNT) data opens up enormous potential for economic growth, reduced inequality, and international co-operation. Access to Global Navigation Satellite System (GNSS) has become a fundamental expectation and mainstay of the modern world. The COVID-19 pandemic has not reduced our dependence on GNSS signals – in fact, it could be argued that the pandemic has made the task to secure or protect our GNSS signals even more urgent.

Increase in GNSS Spoofing Incidents

During 2019 and 2020, there were concerning rises in the number of spoofing incidents worldwide. Several of those incidents have had widespread impacts, including, for example, the reported spoofing of commercial shipping in the Black Sea [2] in which hundreds of ships were affected and the "crop circle"-like spoofing of civilian vessels near the port of Shanghai on the Huangpu River [3]. Circular type spoofing has also been reported by several users in the city of Tehran, Iran [4]. These incidents affected a significant number of commercial users, although the exact motives for these particular spoofing incidents remain unclear. GNSS receivers are subject to a wide range of specific vulnerabilities, but spoofing is perhaps the most insidious of those vulnerabilities, given the potential impacts that a successful zero-day type attack might have on safety- or liability-critical applications, especially if it is part of critical national infrastructure.

As it seems that the chances of encountering a spoofing signal in the real world are increasing, there is a need to understand how receivers will respond to the types of threat they will typically encounter. There is also a need to understand how difficult it is to carry out a spoofing attack on user equipment in the real world. Whilst attention is (rightly) focused on the experience of users who have suffered unwanted consequences from real world spoofing attacks, such as those reported above, it is also worth noting that in these areas there are large numbers of GNSS users who may not have been affected at all by the spoofing activity.

More Scientific Data Needed

Most evidence of spoofing in the real world is anecdotal. The majority of reports understandably refer to the impact experienced by the user – for example, a vessel's position being wrongly reported as being on land when it is actually at sea, or offset by several nautical miles from its true position – rather than the technical measurements or observations that help to assess equipment behaviour. The need for quantitative data to help understand receiver resilience and robustness to spoofing attacks is clear.

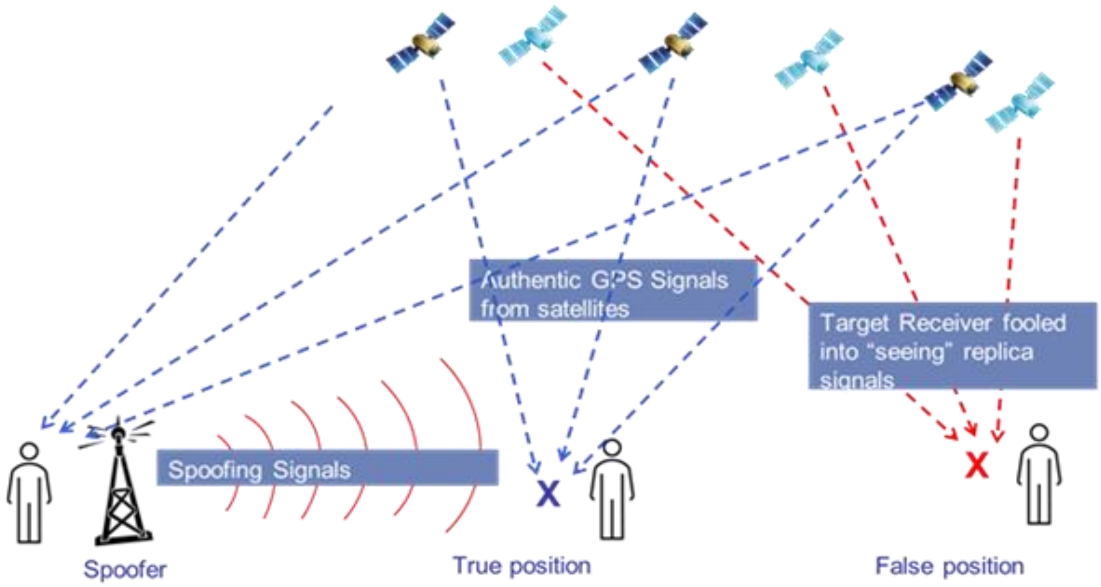
Authentic GPS Signals from satellites
Target Receiver fooled into "seeing" replica signals
Spoofing Signals
Spoofer
True position
False position

Figure 1: Principles of GPS Spoofing

II. How GPS Spoofing Works

In a classic spoofing attack, fake signals are generated from a spoofer located on the ground. The spoofing signals are generated so they are well aligned (overlapping) in the correlators of the target receiver, then "moved off" to a fake position once the receiver has locked on to the spoofer's signal. In the earlier referenced spoofing incident in the Black Sea, the spoofer broadcast fake GPS signals that coincided with the location of a nearby commercial airport if a receiver locked on to them. This may have been an attempt to trick any drones flying near sensitive locations to believe they were located in a restricted area, and cause them to shut down or land. This is "brute force" spoofing where the spoofer transmits signals at a relatively high power level. If a receiver locks onto the spoofer's peak in the correlator, it is spoofed.

It should also be clear that although we have given some examples of scenarios where a receiver reports an incorrect position whilst being spoofed, spoofing can just as easily be applied to timing data. Users relying on precise timing from GNSS satellites also need to be familiar with GNSS spoofing and mitigation strategies to increase robustness and resilience.

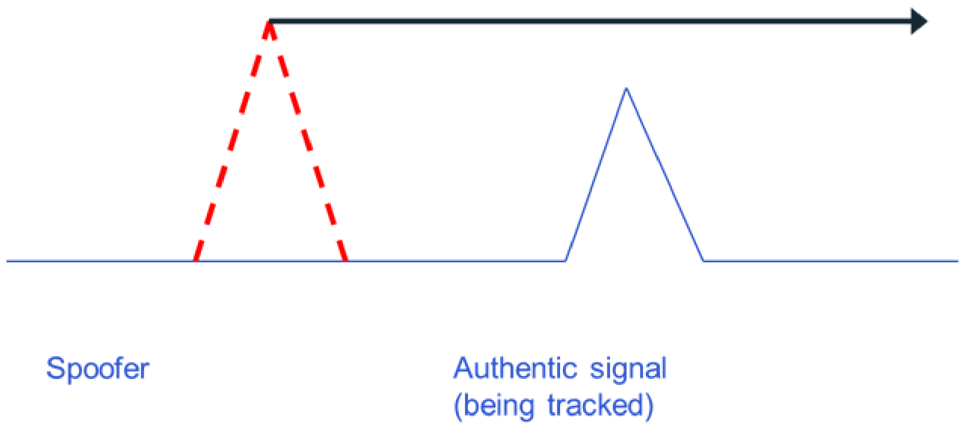

Figure 2: Spoofing in the Correlator

The Test Set-Up and Scenarios

To try to better understand the behaviour of receivers when subject to simple spoofing scenarios, we set up an example where a receiver was subject to GPS spoofing at locations of 10, 50 and 100m distance from the ground truth position. The aim of this spoofing was to induce target receivers to report a position coinciding with the spoofer rather than the ground truth location. During the tests, the power level of the spoofers was ramped up gradually.

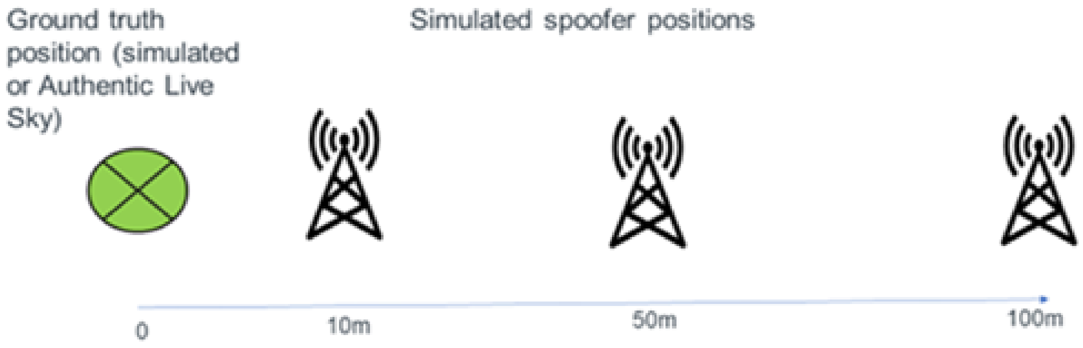

Figure 3: GPS Spoofing Scenarios

Firstly, the tests were carried out using simulated GNSS – in other words, a GNSS simulator was used to generate the live sky and spoofed signals. This set of tests was designed to look at the robustness and resilience of GNSS receivers to spoofing attacks.

Another set of tests was then conducted to examine the difference between testing using simulation only and a situation where Authentic Live Sky GPS signals were introduced into the set-up with only the spoofed signals being generated by the simulator.

Simulation Only Test Results

In the first set of simulation only tests, three sample representative GPS receivers were used. Plots of Horizontal Positioning Error (HPE) and the RMS of the residuals were plotted. Plots for the 50m case are shown below. In these particular experiments, the spoofer power level was ramped up gradually to a maximum, then slowly reduced to its starting point. Data is plotted separately for the ramp up and ramp down in power levels.

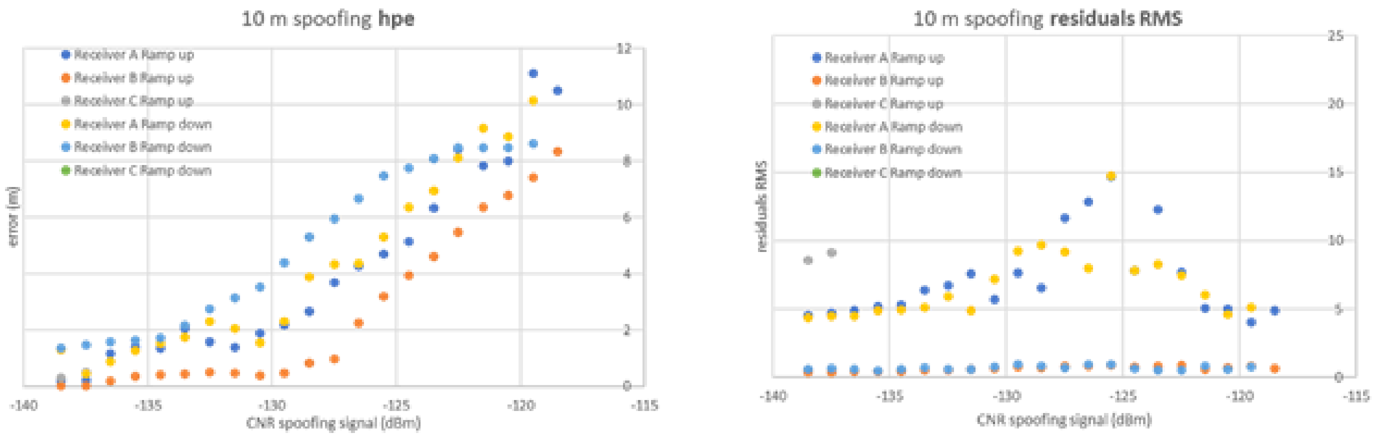

Figure 4: HPE and RMS residuals plot for spoofing attack at 10m

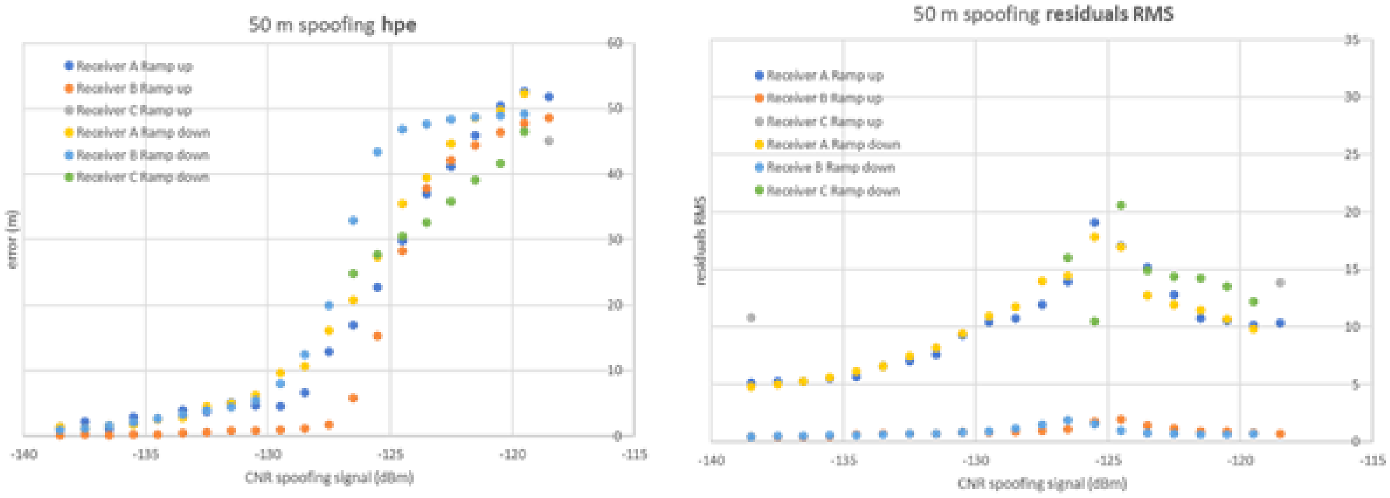

Figure 5: HPE and RMS residuals for spoofing attack at 50m

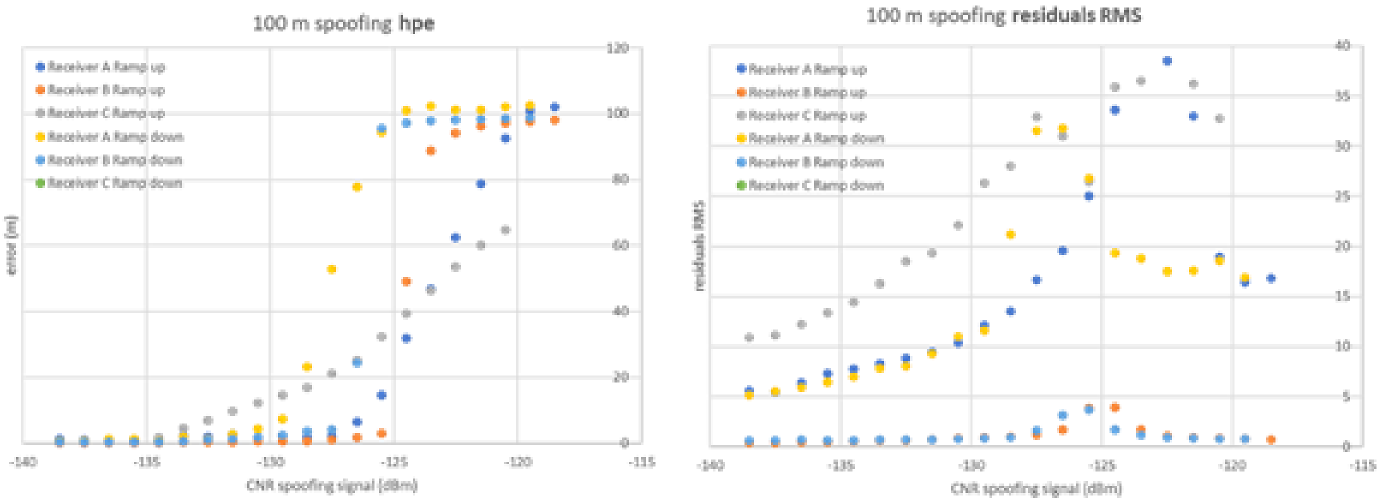

Figure 6: HPE and RMS residuals for spoofing attack at 100m

Discussion of Simulation Only Test Results

The main aim of this paper is to examine the suitability of this type of scenario as a benchmarking test, rather than to provide insights into the behavior of the receivers under test. However, in Figures 4-6, which are plots of HPE and RMS residuals generated from the receivers under test, it can be seen that even when subject to the simple and non-dynamic spoofing scenario used here, the three sample, representative receivers exhibited markedly different behavior. It is also worth noting that the test results from this scenario show the degree to which a receiver can withstand an attack does not necessarily correspond to the degree to which a receiver recovers to its original operating state following an attack. Receiver C struggled with the scenarios. Receiver C often quickly lost lock of the authentic signals and started to report erratic HPE data, failed to recover completely on ramp down, and did not lock onto any transmitted signals regardless of authenticity.

Receivers A and B show good correlation between the point at which the HPE transitions from minimum to maximum as the spoofer power is ramped up, or vice-versa when the spoofer power is ramped down.

The peak in RMS residual appears to flag the point where the solution begins to be dominated by spoofing signals. Note that Receiver B performs significantly better than Receivers A and C at all ranges when it comes to RMS residuals with much lower values consistently, although small peaks in the RMS values can be observed on the 50 and 100m distance runs. Also when the power of the spoofer is ramped down, a peak in RMS residuals is also observed at the point where the truth signal again becomes dominant.

Simulated Only vs Authentic Live Sky Spoofing

None of the sample groups used in the experiments were robust against the spoofing attack, although some receivers were obviously more resistant than others. In these cases, the replica signals required a higher power level before locking onto the fake signal.

However, where the “live sky” and replica signals are both generated by a single RF Constellation Simulator, the conditions for a successful spoofing attack are perfect – with the “live sky” and fake signals perfectly aligned in the target receiver’s correlators and environmental conditions for both signal types also identical. This sort of test is ideal for determining the impact of a “worst case” spoofing attack on a system or device, to understand questions relating to the difficulty (or lack of) in spoofing devices or systems in the real world, or modelling the probability that a system or device could be spoofed. A test set-up is required that allows real world signals to be used in the test set-up. At the same time, the spoofing signal should be confined to a properly screened laboratory.

Test Set-up for Comparing Simulated Only Against Authentic Live Sky Spoofing

Spirent devised a test set-up where authentic GNSS live sky signals are fed into the laboratory, then fake signals are combined with authentic signals in a conducted test set-up. Whilst such a set up constrains the geographic location of a test and its repeatability, it allows for the introduction of authentic GNSS signals that are not ideally aligned with the fake ones and are subject to the real-world environment. It was decided to recreate a very similar set of spoofing/meaconing scenarios to those tested in [5], this time conducting the experiments using both simulated and authentic GNSS "live sky" signals in the tests.

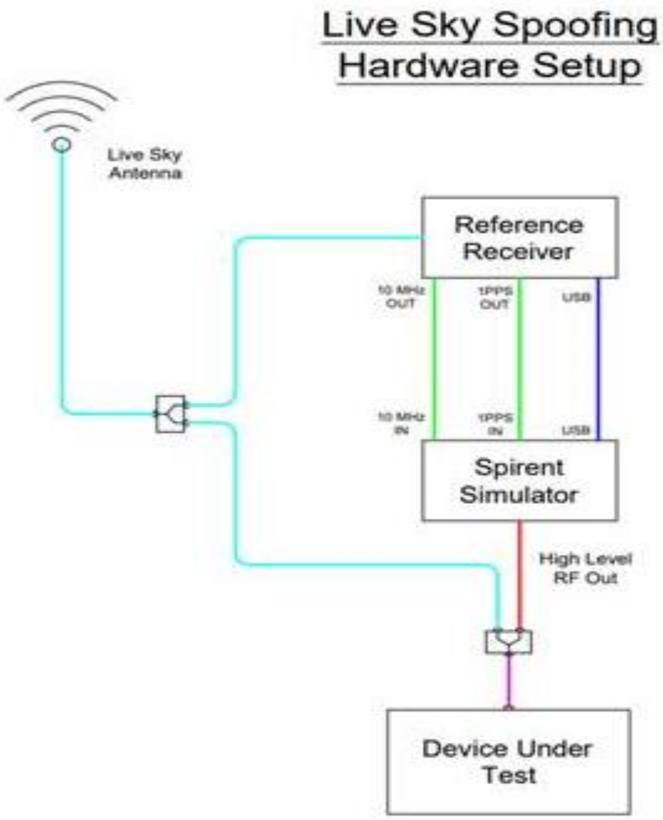

Figure 7: Authentic Live Sky Test Set-Up

Limitations imposed by the Covid-19 Pandemic

Covid-19 restrictions imposed some limitations on the test. The authentic live sky spoofing test could not be carried out at our laboratory site – instead had to be performed at the home of one of the authors.

As a result, the tests had to be compared with the simulation only data that used the Paignton laboratory location as ground truth. Also we were only able to obtain two sample receivers (R_1 and R_2) to undertake these tests.

Results of the Simulation Only and Authentic Live Sky Spoofing Comparison Tests

The reported ground tracks of the two receivers are shown in Figures 8 and 9 for the 50m test case. Figure 8 shows ground tracks for the test case with the simulation only, and Figure 9 shows ground tracks for the test case with authentic live sky and a simulated spoofer. For these particular tests, the spoofer power ramp was amended. We were only interested in obtaining data for the case of an increasing power ramp on the spoofer which was increased at 1dB per minute. Where authentic live sky signals were used, the receiver was allowed to stabilize for 10 minutes before the power ramp was introduced. R_1 reported ground track data is plotted in red, R_2 data is plotted in blue.

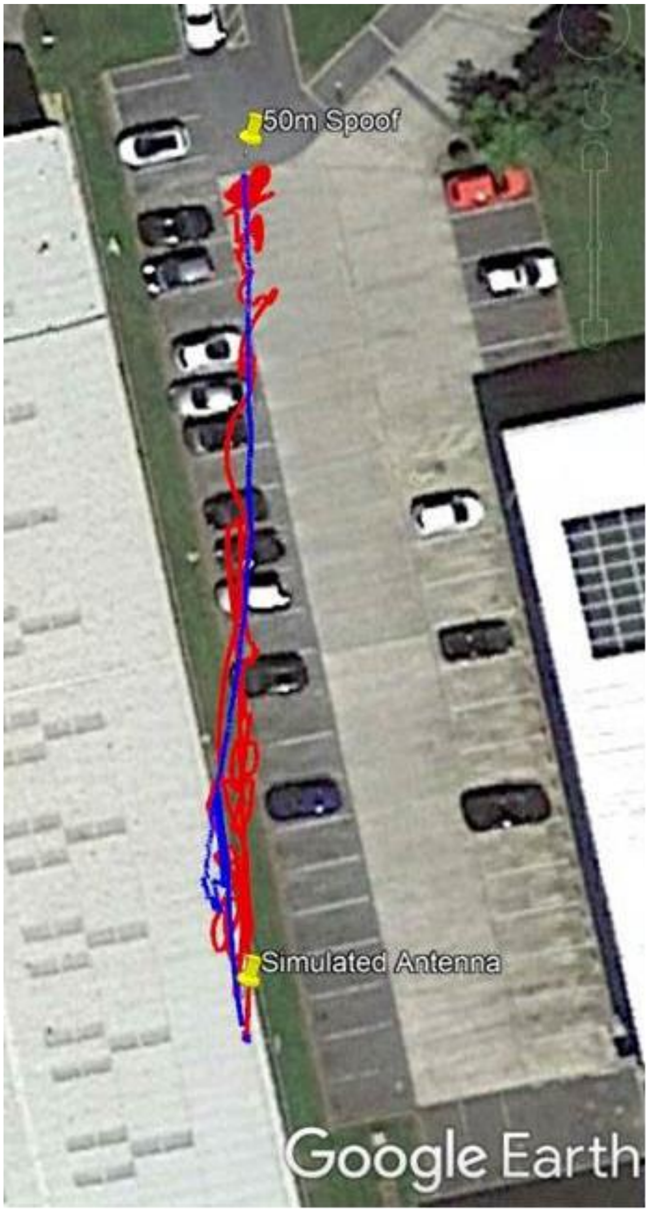

Figure 8: Reported ground tracks of R_1 (red) and R_2 (blue) during the 50m test case (Simulation only).

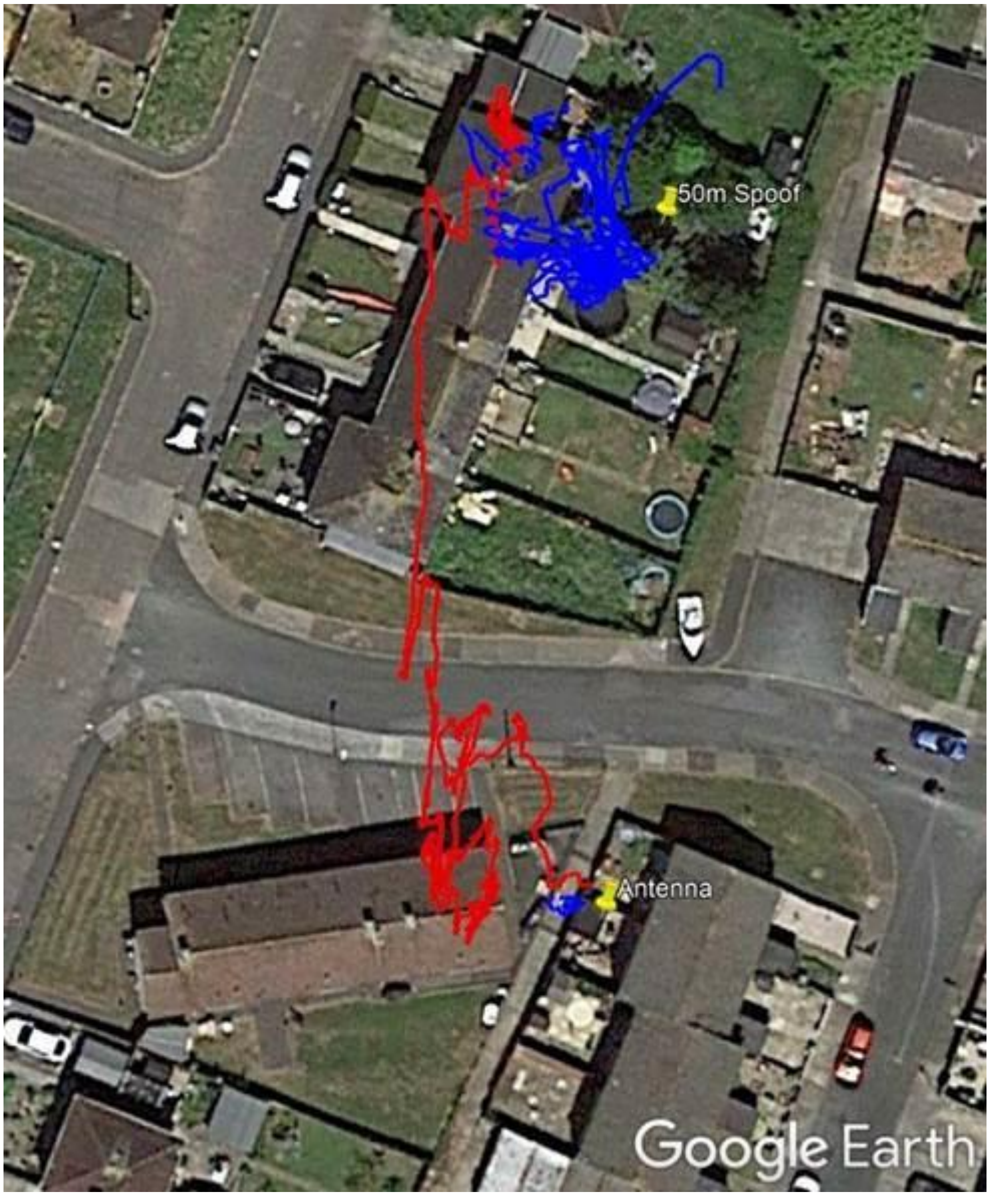

Figure 9: Reported ground tracks of R_1 (red) and R_2 (blue) during the 50m test case (Authentic Live Sky, Simulated Spoofer)

Discussion of Simulation Only and Authentic Live Sky Spoofing Comparison Tests

These results demonstrate the difference between a simulation only test in which a GNSS simulator is used to generate live sky and spoofer signals, and an authentic live sky test in which the simulator is used to produce the spoofed signals only while the receiver is tracking authentic live sky GNSS signals at the test location. Sudden jumps or discontinuities in the reported ground track are more apparent in the authentic live sky tests (especially for R_2).

The increased difficulty in predicting the outcome of a spoofing attack in an urban environment compared to a simulation was expected, as an urban environment is more complicated and dynamic.

III. Conclusion

There are a number of obvious advantages and disadvantages to using authentic live sky signals in this kind of test. While the use of authentic live sky signals is likely to provide a much more realistic test in terms of receiver robustness to a spoofing attack, the results are not easily repeatable as they depend on the satellite geometry and multipath environment at the time of the test. Tests cannot be set up to occur at other geographic locations or specifically set up for satellite geometries of interest.

On the other hand, in the simulator only case, tests are repeatable and can be set up to occur in other virtual locations, at any date or time desired, and for particular satellite geometries of interest. However, as both authentic and spoofed signals may be aligned perfectly at code and carrier level in the receiver, a simulated spoofing attack is much more likely to compromise the receiver under test.

This leads to the conclusion that both authentic live sky and simulator only testing should be carried out when assessing GNSS receivers for spoofing resilience. The authentic live sky tests can provide quantitative data on a receiver's capability to resist a spoofing attack in a representative real-world environment, whereas the simulated only test can be used to perform "worst case" tests and to evaluate the impact of a successful spoofing attack.

It is often much harder to spoof a GNSS receiver in real life than it is when carrying out simulated testing as environmental variables, such as multipath aid the defender in this regard. However, if a spoofer is designed to target a particular position and a receiver passes over that position, then it is often spoofed or severely affected by the spoofing signal – this is why meaconing of the type carried out in the Black Sea or near the port of Beijing has been particularly effective. Spoofing becomes much easier if a receiver is in acquisition or reacquisition mode rather than tracking carrier and code.

The U.S. Department of Homeland Security (DHS) has recently published Issue 1.0 of a Resilient Positioning Navigation, and Timing (PNT) Conformance Framework [6] which defines five levels of resilience from level 0 (non resilient) to level 4 (highest level of resilience).

Categorizing the resilience of equipment and systems within this framework will require a comprehensive test methodology to support it. One important part of that framework will be concerned with establishing the resilience (including resistance) of GNSS dependent equipment and systems to spoofing attacks. In turn, this will require a set of realistic GNSS spoofing scenarios to be developed as benchmarking tests. The work described in this article has been undertaken to better understand the test methodologies and techniques needed to quantify the effects of spoofing on user equipment and systems.

Further Work

More testing needs to be conducted to confirm these findings as the testing of GNSS spoofing attacks introduces a high degree of complexity into the test set-up and small changes in starting conditions can result in marked variations in the end result. Statistical confidence in the results will be necessary and this implies that each test case will need to be repeated to a sufficient degree that allows meaningful conclusions to be drawn. Subjecting a wider range of GNSS receivers to these test scenarios and to carry out authentic live sky scenarios with receiving antennas situated in a wider range of representative environments is clearly desirable.

About the Authors

Guy Buesnel *has more than 16 years of experience working on Robust and Resilient Position Navigation and Timing, having started his career as a Systems Engineer involved in developing GPS Adaptive Antenna Systems for Military Users. Guy has been involved in GPS and GNSS Receiver System Design with the aim of designing a new generation of Rugged GNSS Receivers for use by Military and Commercial Aviation Users. Guy is a Chartered Physicist, a Member of the Institute of Physics and an Associate Fellow of the Royal Institute of Navigation.*

Mark Hunter*, after gaining his honours degree in '94 in Electrical and Electronic Engineering from Brunel University, he travelled far and wide as a contractor working in several Network Operation Centres and helping commission the fibre optic backbone of the internet. The dot com crash soon put an end to that so he returned home, only to find a company called Spirent where he has been ever since. After cutting his GNSS teeth in the UK as an Applications Engineer, he then relocated to the USA supporting this region. In 2016 the opportunity then arose to return to the UK and head up the newly formed Professional Services team, a role that he still enjoys.*

Dan Martin *started his GNSS career working in the hardware team within Spirent, joining the Professional Services team in 2019. He has gained experience working to develop PNT solutions for a wide range of customers and has professional interest in GNSS spoofing and meaconing, and particularly their impacts in the commercial sector. Dan is also focused on developing assessment tools and techniques to aid in the mitigation of spoofing.*

References

[1] F.Filipi, M.Hunter, G.Buesnel, Under Attack – Receiver Response to Spoofing: Robustness vs. Resilience, Inside GNSS, 30 Sep 2020.

[2] M. Jones, Spoofing in the Black Sea: What really happened? GPS World, 11 Oct 2017.

[3] Sinister Spoofing in Shanghai, Inside GNSS, 10 Dec 2019.

[4] GPS World https://www.gpsworld.com/gps-circle-spoofing-discovered-in-iran/.

[5] An Assessment of GNSS Receiver Behaviour in Laboratory Conditions When Subject to Meaconing or Spoofing Scenarios, M.Hunter, F.Filipi, G.Buesnel, ION GNSS+, 25 Sep 2020,

[6] https://www.dhs.gov/sites/default/files/publications/2020_12_resilient_pnt_conformance_framework.pdf.

ICAO Space-WX Advisories – in the Ops-Manual! First Thoughts

Klaus Sievers & Ralf Parzinger
VC, Germany
Klaus.Sievers@VCockpit.de

I. Introduction

Over decades, aviation has relied on crucial weather information provided in standardized form by the Meteorological Authorities of the Worlds´ countries. This may be simple text messages regarding temperature and wind, or huge databases of digital information about the state of the atmosphere, like air pressure, turbulence, jet streams and thunderstorms. A crucial component has been missing, that is information about emissions from the sun that can disturb the ionosphere, increase the radiation dose to people who fly and disturb electronic systems. An in-depth look at Space-Wx was published by the Infrastructure Research Group in the January 2020 issue of the IRRR (https://carleton.ca/irrg/wp-content/uploads/VOL-1-ISSUE-9_FINAL-VERSION.pdf).

After a long consensus building process, a winding road to success, ICAO provisions for Space Weather Advisories were introduced, effective November 2018. Since November 2019, three Global Space Weather Centers have become operational. They monitor the solar and ionospheric activity 24/7, and will provide Space Weather (SWx) advisories when required.

The space weather advisories use existing aviation channels, similar to SIGMET, to make the advisories available directly to aircraft operators and flight crew throughout the flight similar to standard meteorological information. The European Cockpit Association (ECA) reported on this: https://www.eurocockpit.be/news/space-wx-icao-radar-screen.

The advisories provide the most up-to-date information possible on space weather conditions likely to impact aviation and cover these four categories:

a) *Shortwave communications*

b) *GNSS*

c) *Increased solar radiation*

d) *Satellite communications*

ICAO DOC 10100, Manual on Space Weather Information in Support of International Air Navigation, describes the hazards of space-wx in detail. It mentions:

a) *Unexpected loss of communications on shortwave radio (HF) or via satellites*

b) *Problems with navigation and surveillance due to GNSS (Global Navigation Satellite Systems, e.g. GPS, GLONASS) being affected by sporadic loss-of-lock of GNSS, especially near the equator and post-sunset;*

c) *Space radiation effects on electronics, which may result in reboots and anomalies; and*

d) *Issues related to radiation exposure by aircrew and passengers.*

There is almost no guidance material available regarding the practical use of these advisories. EASA, for example, has not yet transposed the ICAO texts, which introduced Space-Wx into its material, although it is already 2021!

Some airlines, such as DELTA and United Airlines, already have Space-Wx in their manuals. However, few airlines consider the new ICAO SWx advisories in their operations. As a first step, some commonly used procedures for failures and the guidance available are put together here to form a set of procedures that might be used to deal with Space Weather Advisories. Procedures such as these need to be in the airlines´ operations manuals, so that both dispatchers and pilots have a common understanding of how to handle SWx Advisories.

II. Recommended Procedures to be Considered With Regards to SWx Advisories

With regards to GNSS, a look into the European GNSS Reversion Handbook for Performance Based Navigation (PBN) Operations [4] Appendix 1, is recommended. It shows that GPS unavailability either impacts or makes unusable the following aircraft systems, depending on installation: GPS receiver / loss of position and time information to aircraft systems, Flight Management Computer (FMC) degraded, operating then by reverting to other methods of electronic navigation or the Inertial Reference System of the aircraft.

Other unusable systems include the ground-based augmentation system for precision landing (GBAS), the satellite based augmentation system (SBAS), Synthetic Vision, Automatic Dependent Surveillance-Broadcast (ADS-B), Automatic Dependent Surveillance - Contract (ADS-C), controller-pilot data link communications (CPDLC) (unusable due to unreliable time-stamp on messages), satellite communications (SATCOM), and the enhanced ground proximity warning system (EGPWS) (if no position-updates from Inertial Reference Systems (IRS) with radio updating). It is possible the airborne collision avoidance system (ACAS-X) may also be unusable, or degraded, due to lack of ADS-B system input. Other degraded systems include: air traffic control (ATC) transponder downlink parameters, ACAS (radio frequency (RF) reducing function, ACAS will work), aircraft communications addressing and reporting system (ACARS) (no position reporting), attitude and heading reference system, emergency locator transmitter (ELT), and digital flight data recorders.

Bottom line, for pilots: Loss of GNSS for navigation and time are extremely serious issues and need to be treated with caution. The following procedures might be of help:

SWx Advisory	Inflight / en-route	Dispatch / before departure
GNSS MODERATE	-Check means of navigation, including distance measuring equipment (DME) (check it is updating), Inertial Reference System (IRS), VHF Omnidirectional Radio Range (VOR) -Check the capability and requirements of the Area Navigation (RNAV) and/or Required Navigation Performance (RNP) systems -Check if conventional approach procedures at destination and alternate can be used and plan accordingly	- Check means of navigation, including DME (check it is updating), IRS, and VOR, including the minimum equipment list (MEL) - Check the capability and requirements of the RNAV and/or RNP - Check if conventional approach procedures at destination and alternate can be used and plan a 2nd alternate - Consider adding 30-minute contingency fuel for unforeseen events, e.g. airspace closures
GNSS SEVERE	- Check means of navigation, including DME (check it is updating), IRS, and VOR - Check if conventional approach procedures at destination and alternate can be used and plan accordingly - Assure availability of planned route / RNAV/RNP - Consider diversion & landing at enroute airport	- Check means of navigation, including dme (check it is updating), IRS, and VOR, including MEL - Check if conventional approach procedures at destination and alternate can be used and plan a 2nd alternate - Check airspace and route availability (RNAV/RNP) - Consider including 1-hour contingency fuel for unforeseen events e.g. airspace-closures - Consider flight cancellation

Degradation or un-usability of shortwave radio communications can have serious consequences, especially if HF is the only communications medium. Air Traffic Control does simply not work without communications, and thus, the following is suggested:

SWx Advisory	Inflight / en-route	Dispatch / before departure
HF MODERATE	- Check conditions on all frequencies in the area, use the best - Use datalink or SATCOM voice if required	- Provide list of best HF frequencies - Ensure SATCOM is available, no MEL exception - No dispatch into areas where HF is prime means of communications - Consider adding 30-minute contingency fuel
HF SEVERE	- Check conditions on all frequencies in the area, use the best - Use datalink or SATCOM voice if required - If no VHF or SATCOM available and HF is only means of communication: do not enter area of HF SEV conditions - Follow communications failure procedures until VHF contact is restored	- Do not dispatch into an area with observed or forecast HF severe conditions where HF is required for communications - Consider adding 30-minute contingency fuel

When flying, it is normal to be exposed to radiation coming mostly from space and, to a lesser degree, from the sun. During rare periods, solar activity predominates and increased radiation levels prevail. To follow the radiation protection principle of ´ALARA´, as low as reasonably achievable, and to help ensure that the radiation dose for both the travelling public and the crew stays within limits, the procedures below are suggested. Note that a reduction in flight altitude by 7000 ft may reduce the radiation dose by half. Details are available in the IFALPA Briefing leaflet [2].

	Inflight / en-route	Dispatch / before departure
RADIATION MODERATE	-Do not perform any planned step-climbs -If above flight level (FL) designated in RADIATION MODERATE message, request descent to 3000 feet below that FL using normal procedures	-Restrict max FL to 3000 feet below FL designated in RADIATION MODERATE message. -Apply until 12 hours after last message
RADIATION SEVERE	-If above FL designated in RAD SEVERE message, request descent to 3000 feet below that FL using normal procedures -If no clearance available within 30 minutes, consider descent with 1000 - 1500 feet / minute to 3000 feet below RADIATION SEVERE Message FL	-No dispatch into areas with RADIATION SEVERE messages -Apply until 12 hours after last message

III. Conclusion

To conclude, we would like to emphasize that Space-Wx is a complex field, with potentially severe impacts on safety of flight operations. ICAO SWx advisories are needed for effective mitigation, and pilots have a key role in this. Mitigation is best performed when procedures for dealing with SWx advisories are in the airlines´ Operations Manuals.

About the Author

***CV Klaus Sievers** flew commercial aircrafts for Lufthansa, starting in 1979; then from 1987 to 2016 the Boeing 747. Klaus is a member of Vereinigung Cockpit (VC, a German Airline Pilots´ Association), an expert on weather for ECA (European Cockpit Association) and a Member of the ICAO Meteorology panel. Klaus is also an Expert Advisor to the Hong Kong Observatory.*

Special interests include weather information in the cockpit, volcanic clouds and space-weather.

References

[1] ICAO, Cross Polar Working Group 2019
https://bit.ly/3deDRYc

https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/mission_support/ato_intl/documents/cross_polar/CPWG27/CPWG27_ICAO_SWX_Advisory_Brief.pdf

[2] IFALPA Human Performance Briefing Leaflet: Aircrews and Ionizing Radiation
https://www.ifalpa.org/media/3467/19hupbl01-aircrews-and-ionizing-radiation.pdf

[3] Australian Bureau of Meteorology, Space Weather Advisories
http://www.bom.gov.au/aviation/data/education/space-wx-advisories .pdf

[4] European GNSS Contingency / Reversion Hand-book for PBN Operations, PBN HANDBOOK No. 6
https://www.eurocontrol.int/archive_download/all/node/12154

[5] DELTA Airlines, Space Weather Workshop, 2017
https://www.swpc.noaa.gov/sites/default/files/images/u33/%281140%29%202017%20SpaceWx%20Workshop-Delta%20Presentation-03May15.pdf

[6] United Airlines, Annual Meeting, American Meteo-rological Society, 2021
https://ams.confex.com/ams/101ANNUAL/meetingapp.cgi/Paper/381920

Integrating Big Data to Understand Crisis Communication: Lessons Learned from Hurricane Maria

Xianlin Jin, Ph.D. (MA, Arizona State University)
Candidate, College of Communication and Information
University of Kentucky, Lexington, KY, USA. ORCID: http://orcid.org/0000-0002-7691-2984
Email: xianlinjin@hotmail.com

Acknowledgment

This article is built on discussing the findings of the following publication: Xianlin Jin & Patric R. Spence (2020). Understanding Crisis Communication on Social Media with CERC: Topic Model Analysis of Tweets About Hurricane Maria. *Journal of Risk Research*.
doi: https://doi.org/10.1080/13669877.2020.1848901.

I. Introduction

Although research has suggested the incorporation of social media into crisis and emergency management strategies, it remains a challenge for practitioners to understand the complex and unstructured social media messages, identify crisis communication patterns, then build their social media strategies. This article highlights utilizing topic modeling analysis to understand crises and disasters' communication patterns that emerged from Twitter across crisis phrases. Particularly, this article reviews and summarizes Jin and Spence's (2020) publication which utilizes topic modeling analysis to explore communication content and social media use during the initial, maintenance, and resolution phases of Hurricane Maria. Integrating big data tools, such as topic modeling, will offer more thorough insights about crisis communication during a natural disaster by unpacking communication patterns that are less represented in the previous studies. Practical implications for crisis and emergency management and future directions are discussed too.

Keywords: big data, topic model, crisis communication, social media, emergency management

II. Communication Strategies for Different Crisis Stages

Crisis scholars and professionals share an agreement that crisis unfolds with a certain pattern and crisis management plans should cope with such patterns to mitigate loss. According to the Crisis and Emergency Risk Communication Model (CERC), crisis and emergency management institutions need to incorporate different communication strategies to cope with a crisis based on its development phases, including preparation, initial, maintenance, and resolution (Centers for Disease Control and Prevention; CDC 2018). While designing crisis management plans, various stakeholders, such as first responders, crisis and emergency management institutions, governments, media, and communities, need immediate and accurate information to mitigate risk and reduce uncertainty. The escalating communication of each phase adds more challenges to monitoring communication patterns, understanding various stakeholders' concerns, and promptly adjusting crisis communication strategies.

As the CERC model highlighted, crisis communication in the preparation phase should concentrate on testing risk messages, warnings, and plans. For the initial phase when a crisis starts unfolding, communication strategies turn to reduce uncertainty and bolster the stakeholders' perceived control over the crisis by explaining risk and offering recommended actions to mitigate risk. It is worth mentioning that building the credibility of crisis and emergency institutions is key to ensure the effectiveness of crisis communication. Besides these strategies emphasized in the initial event phase, more effort should be devoted to develop interactive communication and offer clear information, including the crisis background, on-going crisis assessments, crisis responses, and recovery efforts. The communication patterns of the resolution phase are characterized as evaluating crisis response and discussing the cause(s), blame, and the responsibility of crisis. The main goal of this crisis communication stage is to improve the understanding of risk, assess the effectiveness of the current crisis and emergency management, and promote a positive institution image. The lessons learned from the current crisis will inform the decision-making of future crisis management plans (see CDC 2018; Jin and Spence, 2020; Lachlan and Spence, 2009; Lachlan et al., 2016; Reynolds and Seeger, 2005).

To meet the nuanced communication requirements for each crisis phase, professionals should understand the real-time communication patterns of crisis, then adjust crisis management strategies. The first assignment of obtaining real-time crisis communication patterns has been a challenge for scholars and professionals. As Jin and Spence (2020) point out, many crisis studies used to ask participants to recall their experience with and responses to crises, such as crisis preparation, evacuation experience, information seeking, and media usage (Spence, Lachlan, and Griffin, 2007). However, people's memory may not accurately reflect their perception and behavior during the crisis. Because uncertainty and fear aroused by experiencing extreme events can impact individuals' memory (Jin and Spence, 2020). The growing usage of social media during crises offers us a new way to monitor real-time crisis communication. Analyzing crisis communication patterns that emerged on social media allows professionals to track real-time crisis communication.

Crisis Communication Patterns on Social Media

Compared to traditional media, social media allows various stakeholders (e.g. ordinary citizens, media, governmental offices, crisis and emergency management institutions, non-profits, and for-profit organizations) to share information and have 'an interactive, collaborative, conversational and community-based' crisis communication (Spence et al. 2015, 172). Within the last decade, the percentage of social media usage among American adults increased from 43% (January 2010) to 72% (as of February 2019, see Pew Research Center, 2019).

Among different social media platforms, Twitter has shown impacts on information seeking, crisis communication, and crisis and emergency management. For instance, Twitter users have communicated crisis information during disasters, such as the Haiti earthquake (Smith, 2010). Recent research reveals that influencers control crisis information flow on Twitter and Twitter users' social media attributes impact their ability to disseminate information, such as having a large number of followers and posting many tweets (see Jin, 2020). These findings suggest the importance of understanding real-time crisis communication patterns that emerge on social media and incorporating social media usage into crisis and emergence management.

Indeed, many organizations have created social media accounts and started using social media as part of their crisis communication and engagement; nevertheless, consistent social media usage remains limited, and effective social media strategies are still not the norm (Jin and Spence, 2020; Xu et al, 2019; Xu, 2020). This may be associated with the difficulties associated with unpacking the chaotic crisis communication that emerged on social media. Social media offers real-time, massive, and unstructured data that is hard for scholars and professionals to absorb. To aid in understanding such unstructured data, this article proposes to integrate big data tools to explore social-mediated crisis communication patterns.

Integrating Big Data to Study Social-Mediated Crisis Communication

Traditionally, researchers conduct content analysis with a limited sample of social media data (eg. selecting tweets with a specific hashtag or from a specific Twitter account) to identify the characteristics of frequently retweeted posts or accounts and understand the major themes that emerged on social media (e.g., Lachlan et al., 2014a; Lachlan, Spence, and Lin, 2014b; Lachlan et al., 2016). Although these studies offered valuable insights on how social media impacts crisis communication, it remains a challenge for us to unpack the chaotic crisis communication patterns based on large and unstructured social media data. Being aware of this challenge, this article proposes to integrate big data tools into studying social-mediated crisis communication.

Recent studies have gradually explored social media impacts on crisis information dissemination and crisis communication patterns with big data tools, such as mapping social media users' positions in certain networks to identify influentials who/that control crisis information dissemination, as well as using topic modeling to discover the major topics of disasters and crisis that emerge from large social media data.

For instance, Jin (2020) utilized social network analysis to identify the top 10 influencers in controlling the crisis information flow of Hurricane Irma, and examine what social media attributes (e.g. the number of tweets, likes, and followers) predict one Twitter account's bridge influence of disseminating information. According to Jin, an influentials' bridge influence is reflected by one's ability to reach other users in the network with the shortest path (betweenness centrality). Particularly, crisis influentials tend to have media backgrounds; additionally, these influentials are usually followed by a plethora of Twitter users, have posted many tweets, and demonstrate more connections with other users (Jin, 2020). These findings illustrate that crisis information is no longer only controlled by media; instead, influentials can impact information dissemination on social media. Jin's study also indicates that integrating big data tools into crisis studies will help researchers and professionals discover the crisis patterns that may not be easily identified with traditional methods.

Topic modeling, as one of the useful big data tools, may help scholars address the challenges associated with sampling and coding while conducting content analysis (Lewis, Zamith and Hermida, 2013). As an unsupervised text analytic tool, topic model analysis first helps scholars and professionals transfer large text data into manageable dimensions, identify semantic relations between terms, and eventually enables one to systematically decipher the hidden meaning of unstructured social media data (Grimmer, 2015; Hofmann, 2001; Jin and Spence, 2020; Valdez et al., 2018; Wesslen, 2018).

Recent studies have used topic modeling to unpack the complex crisis communication patterns of disasters and assist professionals in understanding and monitoring social media impacts during crises (Jin and Spence, 2020; Sadri et al., 2018). For instance, Jin and Spence (2020) conducted a series of topic model analyses to identify the salient crisis topics of Hurricane Maria that emerged on Twitter during the initial / maintenance / resolution phases. The following section summarizes the findings of Jin and Spence's study.

Jin and Spence (2020) collected 16,252 Hurricane Maria related tweets posted in the initial phase, 17,937 tweets in the maintenance, and 12,146 tweets in the resolution phase. These authors conducted a series of topic model analyses and word-cloud analyses with JMP Pro 13.

Crisis Communication Patterns in the Initial Phase

Jin and Spence (2020) identified six major topics from the tweets posted in the initial phase of Hurricane Maria. The first emerged topic was about veteran medical care which highlights that veteran patients in Puerto Rico received support from Veteran Affairs. The second topic focused on resilience stories. Many tweets discussed resuming electricity for hospitals in Puerto Rico. The topic of communication needs emerged as the third topic. Twitter users shared their struggles of connecting with others because of no phone service. It is worth mentioning that a new crisis of airfare investigations rises and makes the crisis communication patterns in the initial phase more complex. Twitter users shared their concerns about evacuation and critiques on the expensive flight tickets. The topic of food and water supplies emerged from the tweets sharing food and water supply information. For instance, FEMA's tweet "Officials in PR/USVI opened up points of distribution where people can get food / water. Locations: https://fema.gov/hurricane-maria" had been shared 649 times at the time of data collection. The last topic of tuition support revealed that some schools waived the tuition for displaced college students to reduce their financial stress (Jin and Spence, 2020).

Jin and Spence's analyses reveal that social media users care about the update of the crisis and requested prompt information regarding crisis responses, such as where food and water supply were located. The request for investigating the airfare price added more complexity to the initial phase. Crisis and emergency management professionals should monitor such crisis communication patterns to adjust their management strategies and cope with the crisis. Resilience was one of the major topics in the initial phase. Sharing resilience stories can bolster the public's confidence in controlling the crisis and thus help reduce their uncertainty and anxiety, which supports the communication advice of CERC (Reynolds and Seeger 2005).

Crisis Communication Patterns in the Maintenance Phase

Jin and Spence (2020) discovered nine topics of crisis communication in the maintenance phase. Firstly, in the maintenance phase, Twitter users shared information about Hurricane Maria's wind speed and scale. The public was also concerned about the severity of the crisis. Many Twitter users shared information about the Federal Emergency Management Agency's (FEMA) aid that was delivered to the San Sebastian area. Unexpectedly, many tweets described a story of a mother dog rescuing her child. The medical support topic rises from the story of the United States Navy medical team performing surgeries, which is similar to the veteran medical support topic of the initial phase. Fundraising for Puerto Rico revealed how different stakeholders (e.g. celebrities and non-profit organizations) financially supported the communities impacted by Hurricane Maria. The topic of relief efforts included information regarding water, electricity, and telecommunication recoveries. The stories about the United States Border Patrol, airlines, and marine operations efforts to assisting hospital evacuations were salient on Twitter. The last major topic of clean water emerged from the stories of the United States Environmental Protection Agency (EPA), FEMA, and the government-owned water corporation in Puerto Rico working together to offer clean water for Dorado.

In the maintenance phase, the crisis communication patterns became more complex with most topics that emerged on Twitter. The topic model analysis reveals that Twitter users not only express their emotions and critiques, but also actively seek crisis information, such as information about governments' updates of medical support and evacuations (Jin and Spence, 2020).

Crisis Communication Patterns in the Resolution Phase

According to Jin and Spence (2020), there are five major topics associated with Hurricane Maria in the resolution stage. The first and most salient topic of the resolution phase is food support, which is similar to the topic that emerged in the initial stage. Food had been an issue since the initial phase, which indicates the lack of sufficient food support to the affected communities. The second topic is about the mental and physical health of the victims of Hurricane Maria. The third topic is about deaths caused by Hurricane Maria. People questioned the accuracy of the official death tolls: "Puerto Rican officials have announced a jump in deaths since Hurricane Maria, but the official hurricane death toll is still just 55." The fourth topic concentrated on the insufficient governments' responses to Hurricane Maria. The last topic that emerged on Twitter in the resolution stage was the broken water system in Puerto Rico.

These findings reveal that issues associated with food, water, and medical supports remain unresolved even on the resolution stage of Hurricane Maria. In the early stage of Hurricane Maria, the major concerns were about immediate support, such as food and phone service. While the crisis unfolded, social media users requested long-term and consistent crisis responses, such as addressing the mental health crisis caused by Hurricane Maria and restoring water system victims (Jin and Spence, 2020).

Nevertheless, the government and responsible agencies failed to address the public's concerns and requests. As indicated by the results of topic model analyses, the critiques on the lack of rebuilding efforts were obvious in the resolution phase. Because of the failure of building effective crisis responses across the initial, maintenance, and resolution phases, the public expresses more anger, which may have made the public lose trust in the government's crisis management. These findings illustrate the importance of cooperating social media usage in crisis communication strategies and emergency management plans. In the future, crisis messages should not only address the public's requests regarding crisis management plans (e.g. food and water supplies), but also respond to their emotions and critiques. This study also indicates that integrating big data tools in crisis communication will help professionals to monitor crisis patterns and understand the different stakeholders' concerns and requests. Such knowledge will assist professionals in designing effective communication strategies, implementing pre-crisis and post-crisis management plans, and mitigating the uncertainty of the public.

III. Conclusion

Although crisis scholars and professionals gradually realize the value of social media usage in crisis and emergency management, we still have struggles in identifying the crisis communication patterns from the large and unstructured social media data. This article aims to introduce big data tools to resolve this problem by reviewing and summarizing recent studies that utilize social network analysis and topic modeling to explain the chaotic crisis patterns raised on social media. The article suggests that integrating big data tools in crisis study will help practitioners better understand social-mediated crisis communication and the public's concerns and emotions. Such insights will thus assist professionals in designing effective and interactive communication, offering prompt crisis information and relief responses, and reducing the public's anxiety.

About the Author

Xianlin Jin *(MA., Arizona State University, ORCID: http://orcid.org/0000-0002-7691-2984) is a Ph.D. candidate in Communication Studies at the University of Kentucky. She is also an Integrated Researcher on Disaster and Risk Young Scientist Programme fellow. Xianlin's research primarily focuses on health and risk information seeking, health communication surrounding preventative diseases and environmental health risks, crisis communication patterns, as well as the communication between social robotics and human beings during the risk information seeking process.*

References

Grimmer, Justin (2015). "We Are All Social Scientists Now: How Big Data, Machine Learning, and Causal Inference Work Together." *PS: Political Science & Politics* 48 (1) 80-3. doi:10.1017/S1049096514001784

Hofmann, Thomas (2001). "Unsupervised Learning by Probabilistic Latent Semantic Analysis." *Machine Learning* 42 (1) 177-96. doi: 10.1023/A:1007617005950.

Jin, Xianlin, (2020). "Exploring Crisis Communication and Information Dissemination on Social Media: Social Network Analysis of Hurricane Irma Tweets." *Journal of International Crisis and Risk Communication Research* 3(2): 49–80. doi: 10.30658/jicrcr.3.2.3

Jin, Xianlin and Patric R. Spence (2020). Understanding Crisis Communication on Social Media with CERC: Topic Model Analysis of Tweets About Hurricane Maria. *Journal of Risk Research*. doi: https://doi.org/10.1080/13669877.2020.1848901

Lachlan, Kenneth A., Patric R. Spence, and Xialing Lin (2014b). "Expressions of Risk Awareness and Concern through Twitter: On the Utility of Using the Medium as an Indication of Audience Needs." *Computers in Human Behavior* 35:554-9. doi:10.1016/j.chb.2014.02.029.

Lachlan, Kenneth A., Patric R. Spence, Xialing Lin, and Maria Del Greco (2014a). "Screaming into the Wind: Examining the Volume and Content of Tweets Associated with Hurricane Sandy." *Communication Studies* 65 (5):500-18. doi:10.1080/10510974.2014.956941.

Lachlan, Kenneth A., Patric R. Spence, Xialing Lin, Kristy Najarian, and Maria Del Greco (2016). "Social Media and Crisis Management: CERC, search strategies, and Twitter content." *Computers in Human Behavior* 54:647-52. doi: 10.1016/j.chb.2015.05.027.

Lewis, Seth C., Rodrigo Zamith, and Alfred Hermida (2013). "Content Analysis in an Era of Big Data: A Hybrid Approach to Computational and Manual Methods. "*Journal of Broadcasting and Electronic Media* 57 (1):34-52. doi: 10.1080/08838151.2012.761702.

Pew Research Center (2019). "Social Media Fact Sheet." https://www.pewresearch.org/internet/fact-sheet/social-media/

Sadri, Arif Mohaimin, Samiul Hasan, Satish V. Ukkusuri, and Manuel Cebrian (2018). "Crisis Communication Patterns in Social Media During Hurricane Sandy." *Transportation Research Record* 2672 (1):125-37. doi: 10.1177/0361198118773896.

Smith, Brian G. (2010). "Socially Distributing Public Relations: Twitter, Haiti, and Interactivity in Social Media." *Public Relations Review* 36 (4):329-35. doi: 10.1016/j.pubrev.2010.08.005.

Spence, Patric R., Kenneth A. Lachlan, and Donyale R. Griffin (2007). "Crisis Communication, Race, and Natural Disasters." *Journal of Black Studies* 37 (4):539-54.

Spence, Patric R., Kenneth A. Lachlan, Xialing Lin, and Maria del Greco (2015). "Variability in Twitter Content Across the Stages of a Natural Disaster: Implications for Crisis Communication." *Communication Quarterly* 63 (2):171-86. doi: 10.1080/01463373.2015.1012219.

Valdez, Danny, Andrew C. Pickett, and Patricia Goodson (2018). "Topic Modeling: Latent Semantic Analysis for the Social Sciences." *Social Science Quarterly* 99 (5):1665-79. doi: 10.1111/ssqu.12528.

Wesslen, Ryan (2018). "Computer-Assisted Text Analysis for Social Science: Topic Models and Beyond." *Computation and Language*. https://arxiv.org/abs/1803.11045

Xu, Zhan (2020). "How emergency managers engage Twitter users during disasters." *Online Information Review* 44 (4) 933-950. doi:10.1108/OIR-08-2019-0275

Xu, Zhan., Kenneth, A. Lachlan, Lauren Ellis, and Adam, M., Rainear (2019). "Understanding public opinion in different disaster stages: a case study of Hurricane Irma." *Internet Research* 30 (2): 695-709. doi:10.1108/INTR-12-2018-0517

Back to the Future: Wind Power and the Decarbonization of Shipping

Edward Downing

Marine shipping is undergoing a major transformation as it seeks to decarbonize. Will wind power be part of the solution?

As a significant contributor to greenhouse gas (GHG) emissions, pressure is building on the marine shipping industry to meet ambitious carbon emission reductions of half the 2008 level by 2050. The answer -- as Bob Dylan famously sang -- is blowing in the wind.

Virtually limitless, wind is synonymous with the history of shipping, and an important supplement to other energy sources that could make the industry greener and those carbon cutting objectives achievable. However, with the revival of wind power, engineers and ship designers are harnessing new technologies and materials that provide a more modern take on the cloth, flax, and linen sails on wooden masts of yore.

In their simplest form, modern high-tech sails are arranged on a ship's deck to catch the breeze based on sophisticated computer software. Such a rig can clutter the deck of the ship and interfere with the loading and unloading of cargo. So AirSeas, a spin-off of Airbus Industries, has developed an industrial-scale kite that can pull a ship along without taking up very much room.

There are several takes on reducing the intrusive nature of sails to make them more efficient. Dutch company, eConowind, has developed a highly-efficient suction wing called a Ventifoil which uses an internal fan to enhance the boundary layer of an airfoil to produce more "lift" that drives the ship forward.

Another example, probably the most innovative and widely used wind-driven technology, is the Flettner rotor. These look nothing like a sail and harness the Magnus effect named for the 1850s German physicist. He noticed that when a spinning object – such as a ball – moves through the air, it experiences a sideways force. To capture this effect on ships, giant tubes are mounted vertically on its deck like upright pipes, and a small electric motor gives them their spin. When the wind blows from the side of the spinning rotors, the Magnus effect creates a forward thrust.

There are six ships operating globally with Flettner rotors, including an Ultramax bulk carrier, an oil tanker, ferries, and vehicle carriers, with three more coming on stream later this year. The narrow vertical rotors don't take up too much room and can be mounted on trolleys so they can be moved during loading and unloading operations for cargo ships.

Preliminary estimates of the fuel consumption and greenhouse gas reduction benefits to be gained by retrofitting sails to ships varies from 1% to 47% depending on the number of sails, and the speed and direction of the wind, according to the International Council on Clean Transportation. Usually, the sails are deployed if the wind direction happens to be favourable, but what if ships could take advantage of modern global positioning and weather forecasting technology to plan their routes to maximize the wind? How much greater an advantage could that be?

While these technologies can be retrofitted to existing ships, others have taken a more radical approach. What if the shape and structure of the ship itself was designed to catch the wind? Usually, mariners are fighting against the effects of cross winds, but if the hull of the ship could be designed to act more like a wing, then the ship could literally fly through the wind using its hull as a sail. The International Windship Association says purpose-built wind assisted ships would have a 50% average reduction in fuel consumption and GHG emissions, and some designs could be fully wind-powered.

The shipping industry has serious challenges ahead to reduce its carbon footprint. There are other competing low carbon options under development, but so many of them seem to be focused on finding replacements for traditional fuels. To make a radical change like moving to wind power will require structural changes. Ships are large investments with lifespans of 30 or more years, so ship owners who purchase vessels need to be sure they could share in some of the fuel savings to be gained by the ship operators who lease them to justify the investment. Operators would need to factor limitations on cargo capacity or extended journey times because of wind conditions.

All these problems don’t seem insurmountable given how large the opportunity is, and this time it will be a good thing if history repeats itself so ships are once again powered by the wind.

About the Author

Edward Downing *is the Communications Director at the Clear Seas Centre for Responsible Marine Shipping, Vancouver, BC. Find out more at clearseas.org.*

Recommended Critical Infrastructure Security and Resilience Readings

Felix Kwamena, Ph.D.*
Email: felix.kwamena@carleton.ca

Grezio, A., Babeyko, A., Baptista, M. A., Behrens, J., Costa, A., Davies, G., Thio, H. K. (2017). Probabilistic Tsunami Hazard Analysis: Multiple Sources and Global Applications. Reviews of Geophysics, 55, 1158–1198. https://doi.org/10.1002/2017RG000579

Eastwood, J. P., E. Biffis, M. A. Hapgood, L. Green, M. M. Bisi, R. D. Bentley, R. Wicks, L. A. McKinnell, M. Gibbs, C. Burnett (2017). The Economic Impact of Space Weather: Where Do We Stand? Risk Analysis, 37(2), 206-218, https://doi.org/10.1111/risa.12765

Eastwood, J. P., M. A. Hapgood, E. Biffis, D. Benedetti, M. M. Bisi, L. Green, R. D. Bentley, C. Burnett (2018). Quantifying the Economic Value of Space Weather Forecasting for Power Grids: An Exploratory Study, Space Weather, 16(12), 2052-2067, https://doi.org/10.1029/2018SW002003

Boteler, D. H. Modeling Geomagnetic Interference on Railway Signaling Track Circuits, Space Weather, Vol. 19, Issue 1, January 2021, https://agupubs.onlinelibrary.wiley.com/doi/10.1029/2020SW002609

ICAO Space WX Advisories Instructions to be Included in the OPS Manual. November 10, 2020 https://www.eurocockpit.be/news/icao-space-wx-advisories-instructions-be-included-ops-manual

What’s the worst that could happen? The world should think better about catastrophic and existential risks - Plans and early-warning systems are always a good idea. Briefing, Jun 27th 2020 edition, and Jun 25th 2020,

https://www.economist.com/briefing/2020/06/25/the-world-should-think-better-about-catastrophic-and-existential-risks?fsrc=newsletter&utm_campaign=the-economist-today&utm_medium=newsletter&utm_source=salesforce-marketing-cloud&utm_term=2020-06-25&utm_content=article-link-1

Cybersecurity for Connected and Autonomous Vehicles, Considerations and opportunities for growth, September 2019. https://www2.deloitte.com/ca/en/pages/risk/articles/cyber-connected-autonomous.html

Under Attack – Receiver Response to Spoofing: Robustness vs. Resilience, INSIDE GNSS, September 30, 2020, https://insidegnss.com/under-attack-receiver-response-to-spoofing-robustness-vs-resilience/

Cybersecurity Profile for the Responsible Use of Positioning, Navigation, and Timing (PNT), Services. https://csrc.nist.gov/publications/detail/nistir/8323/draft

Ismael Arciniegas Rueda and Aaron Clark-Ginsberg, the Downside of a Lean Electric Grid Commentary (The Hill) October 13, 2020, https://www.rand.org/blog/2020/10/the-downside-of-a-lean-electric-grid.html

Russian Propaganda, Domestic Terrorism, America's Electric Grid: RAND Weekly Recap, October 16, 2020, https://www.rand.org/blog/2020/10/weekly-recap-october-16.html

Bilyana Lilly, Joe Cheravitch. The Past, Present, and Future of Russia's Cyber Strategy and Forces, Published in: 12th International Conference on Cyber Conflict (2020). doi: 0.23919/CyCon49761.2020.9131723, RAND.org on October 22, 2020, https://www.rand.org/pubs/external_publications/EP68319.html

Mary Lee, Benjamin Boudreaux, Ritika Chaturvedi, Sasha Romanosky, Bryce Downing. The Internet of Bodies Opportunities, Risks, and Governance, https://www.rand.org/pubs/research_reports/RR3226.html

Quentin Hodgson. Strategies for Minimizing Cybersecurity Risks, RAND.org on February 24, 2021, Cybersecurity

Jacopo Bellasio, Erik Silfversten. The Impact of New and Emerging Technologies on the Cyber Threat Landscape and Their Implications for NATO, Published in: Cyber Threats and NATO 2030: Horizon Scanning and Analysis, Chapter 5, pages 88–107 (2020), Posted on RAND.org on January 12, 2021. https://www.rand.org/pubs/external_publications/EP68433.html

Mary Lee, Timothy Marler, Anika Binnendijk. Now Could Be the Time to Form Policy for Emerging Brain- and Body-Enhancement Technologies, commentary, Real Clear Defense, January 12, 2021 https://www.rand.org/blog/2021/01/now-could-be-the-time-to-form-policy-for-emerging-brain.html

The RAND Blog.
Previous Blog Post: Should Communities Be Concerned About Digital Technologies to Fight COVID-19? Next Blog Post: Preparing for a Post-Vaccine World, Domestic Abuse, the Future of War: RAND Weekly Recap

James Ryseff. COVID-19 Highlights the Shortcomings of America's Digital Infrastructure, commentary, Inside Sources, May 14, 2020, https://www.rand.org/blog/2020/05/covid-19-highlights-the-shortcomings-of-americas-digital.html

Jordan J. Plotnek, Jill Slay. Power systems resilience: Definition and taxonomy with a view towards metrics, https://www.sciencedirect.com/science/article/pii/S1874548221000032?via%3Dihub

**Felix Kwamena*, Ph.D.*

Adjunct Professor/Director
Infrastructure Resilience Research Group (IR^{2}G)
&
Director, Energy Infrastructure Security Division
Low Carbon Energy Sector
Natural Resources Canada

INFRASTRUCTURE RESILIENCE RESEARCH GROUP (IRRG)
UPCOMING EVENTS

2021- 2022

EVENT	DATE / LINK
Training Courses **Watch for new Dates**	https://carleton.ca/irrg/training/ **Suspended Due to COVID -19**
4th International Security and Resilience Symposium **Watch for new Date**	https://carleton.ca/irrg/cu-events/4th-international-urban-security-and-resilience-symposium/ **Cancelled Due to COVID -19**
3rd Economic Environmental Security, and Resilience Workshop Theme: A Multi-stakeholder, Multidisciplinary Approach to Addressing Challenges and Leveraging Opportunities **Watch for new Date**	November 10, 2020 https://carleton.ca/irrg/cu-events/economic-security-resilience/ **Cancelled Due to COVID -19**
2020 IRRG Dean's Lecture The Dean's Annual Lecture Series – Infrastructure Security and Resilience: Economic Security, Resilience. **Watch for new Date**	November 18, 2020 (4:00 PM – 6:30 PM) https://carleton.ca/irrg/cu-events/2020-deans-lecture/ **Cancelled Due to COVID-19**

Check out IRRG's Website for:

Upcoming events

https://carleton.ca/irrg/events/

Professional Training / Development Courses

https://carleton.ca/irrg/training

Latest Issue of Online Journal
***Infrastructure Resilience Risk Reporter* (IR^3)**

https://carleton.ca/irrg/journal/