BLUE PAPER 2-2

The Cascade Effect and Nature of Trust and Hierarchical Structures within the Context of Mass Casualty Incident Management Networks

By Herschel Campbell, Ronald Reagan Research Fellow

Part 1: Understanding the Cascade Effect: Two Personal Examples

Cascade effects are the ramifications from an incident, attack, or event. According to Goldschmitt (2009), "The premise of cascade effects is that the initial attack or event may trigger secondary disasters."[1] These events can be singular or multiple in nature. For instance, a large-scale disaster such as a hurricane could create multiple secondary incidents and complications such as large-scale power outage, massive flooding, or large areas without access to food and water. Each resulting issue could have its own secondary and tertiary issues, constituting what Goldschmitt & Bonvino (2009) characterized as a multiple cascading event.[2] An event can be singular and linear, though this is not as common, an example of which from Goldschmitt & Bonvino (2009) is a communications failure, which could disrupt specific agencies or services, but would be less likely to have the many branch-off effects of a multiple cascade event like those described above.[3] Even singular and linear cascade events could lead to further cascading events and create multiple, branched cascading scenarios.

My title is Global Security Operations Center (GSOC) Analyst, and my job is to monitor multiple business units, assets, and employees, carrying out company contracts and operations in over 70 countries world-wide for a major oil and gas parts supplier in Houston, Texas. In this capacity, we must operate a 24/7/365 operations center. Our emergency operations center planned to have backup and redundant systems in place to ensure communications channels specifically to mitigate a failure in our communications and control (C2) capability that would leave the company executives in Houston largely blind to emerging threats.

To preempt a cascading event, Goldschmitt & Bonvino (2009) recommend the use of either natural or man-made stop "gaps" to "arrest" an event from further cascading.[4] Beginning with the 2015 West African

[1] Goldschmitt, D., & Bonvino, R. (2009). Jerusalem: One of Our Own. In Medical Disaster Response a Survival Guide for Hospitals in Mass Casualty Events. Hoboken: CRC Press. p.71.

[2] Ibid. p.72.

[3] Ibid. p.72.

[4] Ibid. p.73.

Ebola Outbreak, following scenarios give real life examples of the dynamics of cascade effects.

Example 1: West Africa Ebola Outbreak

Because we work in many high risk destinations such as the Niger Delta, off the coast of Liberia, Sierra Leone, and Ghana, the Democratic Republic of Congo, Angola, Saudi Arabia, Egypt, and, until recently Yemen, the ability to quickly relay information from field workers to regional managers and then to the GSOC is imperative in preventing small-scale incidents from becoming multi-aspect crises. Without this ability, miscommunication can result in misrepresentation of the facts, loss of business, placement of assets in unsafe locations, and other wrongful decisions that either place assets in harm's way or unnecessarily cost millions to the company.

Part of my GSOC duties include monitoring events in West Africa; my Area of Responsibility (AOR). Initially, the company did not perceive the Ebola virus outbreak to be a significant issue. Business was limited in West Africa, particularly where the outbreak was occurring, and our focus has always been on the physical security side of things. However, it was my opinion, supported by my superiors that we needed to develop a communications system for monitoring events as a precaution. In this case, we designed and maintained an online slide-deck that gave updates on the border restrictions, case numbers, travel recommendations, advice for reducing risk of infection, and overall threat assessment (pertaining to the Ebola virus) in each country in Africa. The effort proved prudent as cases began to spread and many businesses began fleeing the continent. Our operations continued in all but the worst hit countries and our travelers had visibility and insight into where they could and could not conduct business, travel, and which modes of transportation were available.

This preempted many possible cascading issues including workers getting infected, loss of business, disruption to travel plans (we did have some but not nearly as many as we could have had we not had companywide visibility), and, in at least one case, legal issues, as one traveler wanted to break the restrictions on travel to one African nation. This information would not have been disseminated as quickly or reliably if we had not implemented the slide-deck. Nor would many of the meetings about the issue been scheduled had the company not taken preventive action due to the creation of an information gap between the corporate, regional, and local business units concerning the situation. The creation of the slide deck and the active attempt by the GSOC to promote information sharing, are examples of what are referred to by Goldschmitt & Bonvino (2009) as man-made gaps, which arrested the event from further cascading.[5]

Example 2: UAV Operations

Another example of potential cascade effect comes from my work as a Mission Intelligence Coordinator for the United States Air Force. In this capacity, my responsibility was to serve as a liaison between ground commanders on the battlefield and the pilots and sensors who operate unmanned aircraft. Here the cascade effects from bad information or coordination can be either linear or branched, singular or multiple. For example, lack of coordination could result in wrong or incorrect information, focusing on the wrong target or, in severe cases, firing at the wrong target. The ramifications could be as narrow and singular as wasted mission time or as branched and impactful as disrupting U.S. foreign relations, paying compensation to

[5] Ibid. p.73.

families, damaging U.S. credibility with local nationals, loss of money, loss of assets, and loss of life.

Conclusion: Cascade Effects can be Far Reaching

Goldschmitt & Bonvino (2009) state that "Cascade effects can be immediate or delayed…An excellent example is the struggle of the rescuers of September 11th, as they became ill from diseases that may have been caused by the original event…"[6] In my experience, the Ebola virus outbreak has led to multiple discussions, even months after the worst of the outbreak ended, to decide when it was safe to resume operations. These discussions resulted in our finding that secondary effects like lacking medical infrastructure and poverty impacted the safety in the worst impacted nations. Even months after the worst of the crisis, West Africa is still reeling economically and it affects how we do business. Relative safety of operational areas, access to and quality of medical care, border restrictions and screenings, and transportation availability all impact where and to what extent we can conduct business operations. These ongoing issues in West Africa illustrate how cascade events can have long lasting and far-reaching implications.

Part 2: Understanding How Hierarchical Structures Increase the Need for Trust in Mass Casualty Incident Management Networks

Hierarchical structures refer to those structures that deal with tiered systems of management. A common example might be witnessed in larger businesses such as GE, Ford, Shell, BP, etc., where there are multiple departments, divisions, and levels of management, however any structure which is divided into clear top to bottom levels of division and/or control can constitute a hierarchical structure. For instance, in the GSOC, we have a Director of Corporate Security, then the GSOC Manager, a lead analyst, and finally basic analysts. Each of these tiers has specific responsibilities and rigid relationship protocols with the other tiers. Moynihan (2008), quotes Alter and Hage (1992), who state that "characteristic of networks is that they are not hierarchical, relying on lateral linkages and self-regulation," thus implying that networks are the opposite of hierarchies.[7] This would imply then that hierarchical structures rely on horizontal linkages and tight, rigid regulation. This is also true of my experience. The GSOC is tightly guided by rules set forth and passed down from the Director of Corporate Security and the GSOC Manager.

When it comes to Incident Command System or other mass casualty incident management networks, elements of both hierarchical structures and networks are combined. The hierarchical and rigid aspect of these networks can create issues with trust between workers on the ground who deal with split second decisions and ever changing circumstances and leaders at the top who may appear distant from the immediate situation. As Moynihan (2009) states, "Even though the hierarchical structures that characterize the ICS are designed to manage via authority… trust was still essential in facilitating coordination. Hierarchical structures' and rules meant there was less reliance on trust…"[8]

[6] Ibid. p.75.

[7] Moynihan, Donald P. (2008). Combining Structural Forms in the Search for Policy Tools: Incident Command Systems in U.S. Crisis Management. Governance: An International Journal of Policy, Administration, and Institutions, Vol. 21, No. 2. p.208.

[8] Ibid. p.218.

This is because where networks intrinsically rely on cross coordination and the assumption that elements of different agencies are expert or the lead in their respective areas, hierarchies work in more order and obey, military style directives. This creates an atmosphere of "do it because I told you to" versus trust that each person is a co-equal and brings a unique skill set. The former is not always preferable in a crisis situation where minute-to-minute choices must be made, and such decisions could lead to life or death outcomes. This is because in such instances, workers used to being instructed to blindly follow orders may not have the situational wherewithal or confidence to rely on their skills and make difficult decisions absent direct commands. The danger then becomes workers who chose inaction over making "the wrong decision." Crisis responders in particular need to be able to trust in their decision making, something that is not strongly promoted in hierarchical structures.

The positive aspect of hierarchies is that they can lead to quick decision making provided that a steady communications channel exists between hierarchical levels. For instance, on a battlefield, a commander can give an order and immediately troops, obeying, know what is expected of them and how to react. The negative side of this relationship comes when choices are less clearly delineated. Here we will look at an example from this writer's work.

Facility Fire Demonstrates Need for Trust in Hierarchical Structures

My work uses an ICS style, which combines the horizontal, hierarchical direction of the GSOC mentioned above with linier networking with regional security managers, independent business units, IT, and occasional third party actors.

One instance of possible confusion and trust issues arose early in my work there. There was a facility in the United States that experienced a fire near one of our company's work yards. Because the GSOC was new in its development and had not experienced many events, the fire fell outside of issues that we had traditionally addressed. It took place late in the afternoon, when the analysts were about to leave work, the management had already left for the day, and there was no standing directive on how to address a potential emerging crisis of this nature. Multiple questions needed to be addressed in short order including: was our facility impacted, how many were hurt, what was value of any potential damage, did our employees know about the issue, what missing information did executives need? All of these questions carried consequences for non-action. If we did not know the answers to these questions the company could find itself liable for injury, bad public relations, and the GSOC could look inept. In oil and gas, ineptitude in a business unit (physical security) that intrinsically costs more money than it makes could lead to closure of the business unit. This was a critical test of the GSOC's capabilities early in its creation.

What ultimately saved the GSOC and allowed for a variety of lessons learned and growth points was trust. The structure was hierarchical, but the management practiced a policy of trusting its analysts. In this case, this writer was the one on shift, alone, at the time of the incident. My response was adhoc, and consisted of using what resources we had available to call the emergency services department in the town where the incident occurred, use our communications and technology equipment to identify the facility and research the extent of the fire, and coordinate that information to our executive leadership within a matter of a couple hours. The

results were mixed. We successfully identified that an incident had occurred, however the facility affected was inaccurately labeled as one of ours. In fact, it had been a leased facility from a third party. We did notify the proper executive leadership, which showed that we could respond quickly and disseminate information in a timely fashion, but we were wrong on some of the details. This was both due to a lack of a standard operating procedure (SOP) and lack of experience.

Conclusion: Trust is Essential for Effective Crisis Response

Moynihan (2008) addressed the importance of SOPs, noting, "Task-relevant SOPs reduce uncertainty, disseminate knowledge, and reinforce central control of inter-organizational hierarchies."[9] This was a lesson we learned from this event and, in the coming months, the company made a concerted and ultimately successful effort to develop SOPs.

More importantly however, as in the task force example used by Moynihan (2008), trust was a deciding factor on the GSOC being able to act."[10] It was trust in the hierarchy to allow the analysts to do what they could and trust in our judgment that allowed us to successfully identify the problem. Although there were mistakes, none of the analysts were blamed in the after action report for any of the failures. Instead, there was a team meeting, which led to positive production of the SOPs and lessons learned, as well as the further insight for each of the analysts. We were also able to realize the need for expanded 24/7 coverage. In short, the overarching takeaway was that trust was a necessity in running the GSOC. This same lesson can be aptly applied to any emergency management or crisis department or organization.

[9] Ibid. p.218.
[10] Ibid. p.219.

American Leadership & Policy Foundation

1201 N.W. Briarcliff Parkway
Second Floor, Suite 200
Kansas City, MO 64116

2200 Pennsylvania Avenue
N.W., 4th Floor East
Washington, D.C. 20037

For more information on this paper or similar issues, visit: ALPF.org

About the Author:

Herschel C. Campbell *is a Research Fellow at the American Leadership & Policy Foundation, Global Security Operations Center Analyst for a leading international oil and gas entity, and a former United States Air Force Intelligence Analyst. Campbell has authored and presented assessments and research to the media, academia, private business interests, state and federal leaders on multiple issues to include: defense, EMP, the West African Ebola Crisis, Gulf of Guinea piracy, militancy and terrorism, global security, and specialized intelligence assessments. He holds an Associate's Degree in Intelligence Studies and Technology, Bachelor's in History Education and a Master's in Emergency and Disaster Management from American Military University.*