

## A Preventive Strategy for Possible Attacks Aimed at Crippling the Cyberspace Controlling Food & Water Supplies in HACCP Programs

Mohamad Azzam F. Sekheta<sup>1\*</sup>, Abeer H. Sahtout<sup>1</sup>, Abdel Sattar A. Airoud<sup>2</sup>,  
Mirvana A. Airoud<sup>2</sup>, Farid N. Sekheta<sup>1</sup> and Nela Pantovic<sup>3</sup>

<sup>1</sup>*Sekheta Bros Company, R&D Department, Gdaideh Aida Str.* <sup>2</sup>*University of Parma, Faculty of Medicine, Via Volturmo 39, 43100 Parma, Italy,* <sup>3</sup>*University of Belgrade, Agriculture Faculty, Vasilija Gacese 5A, 11000 Beograd - Serbia*

Critical infrastructures underpin the domestic security, health, safety and economic beside physical and cyber systems include energy production, transmission and distribution, food and water, transportation, telecommunications and information systems. These systems grew up independently, in a world of relative trust. They were designed to minimize occasional failures from aging and degradation, adverse weather conditions, natural disasters and accidental operator error. Over time these systems have become increasingly complex and interdependent, increasing the potential for these occasional failures that the systems were designed to minimize. In general these systems were not designed to withstand terrorist attacks. Large food companies using the internet and other electronic information infrastructure in their electronic systems, have to employ specialists or high skilled people equipped with the tools necessary to conduct computer and computer network investigations in order to protect their "Cyberspace" from being threaten or attacked. This paper has the purpose of examining means of establishing basic prevention, surveillance and response capacities based on the implementation of enhanced HACCP principles focused on detecting and defeating against threats from cyber-sabotage to e-crime and on preventing human exposure wherever possible.

**Key words:** HACCP, cyber-terrorism, cyberspace, information infrastructure, cyber-sabotage, E-crime, computer security.

Increasingly, the modern world depends on computers electronic mail, mobile and many other electronic devices such as faxes, printers and scanners. Using them we can now control the vital infrastructures such as power delivery, communications, transportation, food processes, food and water supplies, aviation, financial services and many others. In food industry, PCs and other above mentioned devices are used to store data and other information concerning food safety plans, HACCP programs and quality control records to business plans to various other vital records. Although Personal Computers (PCs) are good tools, they are vulnerable to the effects of poor design and insufficient quality control, to accident, to the lack of knowledge or skills of their users and perhaps most alarmingly, to deliberate different kinds of attack aimed at crippling the electronic information infrastructure "Cyberspace". In this paper, a novel defeating plan against different threats or attacks on Cyberspace controlling food processing and water supplies based upon the seven HACCP principles is being established including important and helpful recommendations, tips and guidelines in order to implement

HACCP programs more safely and successfully.

### **Cyber-terrorism on Cyberspace controlling Food and Water Supplies:**

Nowadays modern thief can steal much more with a computer than with a gun and perhaps without putting himself into considerable risk. Tomorrow's terrorist may be able to do even much more damage alone with a single keyboard attached to his PC than with a bomb (1). As a matter of fact, all food industries worldwide are at real risk. As the cyberspace becomes increasingly ubiquitous in our everyday lives, the risks that act of terrorism targeted at, or utilizing, Cyberspace grows exponentially. Unfortunately, sabotage of critical systems even for short periods of time can destabilize nations in the global mean, reek huge losses to economies and individuals, cause untold havoc, and threaten innocent lives too.

In general, attacks on food and water supplies, could involve stealing classified files, altering the content of Web pages, disseminating false information, sabotaging operations, erasing data, or threatening to divulge confidential information or system weaknesses unless a payment or political concession is made. Such attacks could also involve remotely hijacking control systems, with potentially dire consequences.

\*Corresponding author, mailing address: Sekheta Bros Company, Food Safety R&D department, Jdaideh, Aida Street 1, P. O. Box: 10405, 21000 Aleppo, Syria. Phone: 00963-94-364053, Fax: 00963-21-2226020. E-mail: [sebc@scs-net.org](mailto:sebc@scs-net.org)

### **The reasons why Cyber-terrorism is being practiced**

Cyber-terrorism could involve destroying the actual electronic machinery of the information infrastructure; remotely disrupting the information technology underlying the Internet, using computer networks to take over machines that control the quality or safety data of food, change data of quality control reports, power plants, or dams in order to wreak havoc or even death to innocents.

There are many reasons why terrorist attacks the cyberspace (2) as such actions are inexpensive, anonymous, low risk, little evidence, difficult to investigate, does not require the possession of contraband and may aggravate the effects of a physical attack.

### **What can people involved do?**

Governments, Health Authorities in cooperation with WHO, FAO, FDA (USA), and many other globally well-known organizations or food manufacturers and scientist dealing with food safety worldwide have to work hard all together on defeating cyber-terrorism affecting the Cyberspace to ensure acceptable safety level to food and water supplies anywhere in the world. It is every one's responsibility; there is a real need to train all people working in food industry but mainly the starters among them especially in the developing countries, on how to practice the standard food safety protocols correctly in order to guard against contamination.

Governments, governmental agencies and other related institutions on the other hand, have to work hard to continue to provide assistance in planning and response to real or suspected terrorist incidents in order to ensure safest food supply. They have to focus on the following major three areas and containment through rapid response:

1. Deterrence can be accomplished by increasing the presence and visibility of inspectors at critical points in the food production and distribution system as well as the water supplies and reservoirs.
2. Surveillance of imported and domestic foods must be strengthened.
3. Threat assessments of the food industries and water supplies are also a key to identifying where the vulnerabilities lie and how to close those gaps.

Still, there are many things food industry managers, food handlers and other workers can do to help insure the safety of the food products they prepare or manufacture. Food industries management (3) therefore should pay considerable attention to all people working in the long food chain in order to know their employees and consider doing background checks and pay attention to their behaviors, restrict facility access, know their contractors and their policies and whether they have free access to all parts of the facility (such as cleaning crew, pest control representative), know their suppliers and the safety of their products and

should be confident and at the end to understand the transport and distribution chain clearly before and after their operation. Changing people's behaviors is only possible to achieve by changing their thoughts, and then to expand their thinking to consider ways to minimize the opportunity for both accidental and intentional contamination of food and water supplies. Special list of emergency contacts and resources must be obtained in each food establishment. In case of being attacked or just a real target for possible attack on its cyberspace, food establishment's management must seek immediate assistance from cyber security experts. Additional aid should be seeking from their local authorities and law enforcement and other emergency response agencies in the country too.

### **Developing a plan for new preventive strategy**

There is a strong parallel between developing a preventive strategy for possible attacks on food and water supplies and developing a hazard analysis and critical control points (HACCP) plan. Both emphasize preventive over reactive measures. Preventive strategy and measures against water supplies and agricultural & food's terrorism must be determined on a case-by-case basis.

Each company or food organization with the aid of external experts and consultants working together with its local HACCP-team and R&D department should evaluate its unique situation at each of its locations and develop a sensible approach for managing risk. Critical factors in developing these preventive measures will include evaluating specific hazards, determining relative risk, and evaluating economic realities. Initially a food company, establishment or organization should complete hazard analysis of its facilities and operations to identify significant hazards and exposure potential and to determine the risks of an occurrence. This analysis should not be limited to the production facility nor limited to peak operating times, but should include other possible hidden or insidious hazards together with the entire scope of operations including the Cyberspace too.

Next, critical control points (CCPs) should be identified and monitoring procedures established for these critical control points. Since it will probably be impossible to eliminate all hazards, a reasonable procedure must be instituted to manage them. Documentation and verification must be part of the protocol.

### **Prerequisite measures for making it works safely**

The key to successful food safety and other HACCP-based programs is vigilance by management and all employees involved. Training is a must. A clear standard operating procedure must be developed and followed for day-to-day operations, for all suspicious incidents, and for actual terrorist and other attacks. The problems resulting from a terrorist attack on the cyber space would be similar to those a food processor might anticipate in its crisis

management plan. When a food product safety is in question, for example, recall procedures would need to be followed:

- Farmers might start by requiring certification from their suppliers and providers periodically seeking third-party verification. Growers can monitor harvests until the product has left their premises.
- To the extent practical, access to cropland and livestock should be controlled and restricted to appropriate personnel. Surveillance equipment is also an option. Consideration should also be given to compartmentalizing livestock operations and requiring foot and even vehicle sanitation dips at critical access points (4).
- Food processors should request certifications from their suppliers and require protected transportation of ingredients. Maintain security and integrity of water supplies.
- Controls during distribution and transit are important. The seal numbers should be communicated electronically, with the numbers and seal integrity verified upon receipt. Off-loading should be conducted under controlled conditions and the process should be monitored periodically.
- Access to processing areas by visitors and employees should be strictly controlled electronically both within the plant and between different areas of the plant.
- Employee and contractor screening will become increasingly important. According to their experiences, authors of this paper recommend that both criminal background and credit checks be conducted as a condition of employment. Individuals purporting to be inspectors should provide appropriate identification and be escorted at all times within the plant.

Employees should be made aware of their responsibilities to stay alert for and report suspicious activities, objects, and people. Employees can also help watch for surveillance of their facilities by suspicious person or party, surveillance of employees at work, presence of unidentified, unattended or unauthorized vehicles, presence of containers in or near facilities and for unauthorized access by any unidentified persons or employees

It is prudent for all food companies to have procedures in place about handling packages or heavy envelopes which arrive in the mail or by delivery services from unknown senders, have unclear return address, and or have unusual odor or appearance.

Management should also file a copy of the company's safety and emergency procedures with the local municipal planning department and with emergency response agencies,

requesting that these documents be printed out and safeguarded together with additional electronic copy and not released to other parties without corporate management's knowledge and consent.

### **Developing preventive strategy based on HACCP principles**

The format of preventive strategy or security HACCP based defeating plans against threats and attacks to food & water supplies aimed at crippling the Cyberspace will vary. In many cases the plans will be product and process specific. However, some plans may use a unit operations approach. Generic HACCP plans can serve as useful guides in the development of process and product HACCP plans. However, it is essential that the unique conditions within each facility be considered during the development of all components of the HACCP plan.

In the following paragraphs, the developed security plan based upon the seven HACCP principles (5) will be outline so it can be developed in order to be implemented more successfully on the Cyberspace as an effective defeating plan against Cyber-terrorism's threats to food and water supplies. Each of these HACCP principles must be backed by sound scientific knowledge.

As we all know, HACCP is a program which helps in identifying the critical control points for successful security plan for defeating threats ranging from cyber-sabotage to e-crime in food establishments and water supplies.

Due to the technical nature of cyber terrorism's threats on the electronic information infrastructure, requirement for skillful computer security advisors is a must in this case. It is recommended that experts who are knowledgeable in dealing with Cyberspace should either participate in or verify the completeness of the hazard analysis and the HACCP security plan.

HACCP team will then establish a flow diagram for the Cyberspace used and then will perform an on-site review of the operation to verify the accuracy and completeness of the flow diagram. Modifications should be made to the flow diagram as necessary and documented. After the preliminary tasks have been completed, the seven principles of HACCP will be applied.

The HACCP team will also determine critical limits, monitoring methods, and any corrective action to be taken.

The success of security HACCP based defeating plans against threats or attacks to food & water supplies aimed at crippling the Cyberspace is dependant upon each one of the specialists of HACCP and employees of the food processing in the organization itself but those who are controlling the cyberspace have the major role in this particular case. Although it is quite hard, but a clear distinguish must be checked and define between real threat and hoax. Responding to false alarms can overwhelm public safety response capabilities, engender a sense of nonchalance after numerous repetitions, incite public fear and anxiety inappropriately and cost money.

In order to develop such plan successfully in a food establishment, we would suggest its local HACCP team to follow these guidelines and tips:

1. Analyze hazards; identify their effective controlling measures.
2. Develop adequate flow diagram for each manufacturing or other process.
3. Modify the flow diagram as necessary; develop adequate records.
4. Examine each step to determine whether there are significant food security hazards. Conducting a hazard analysis evaluates significant hazards and exposure; determine risk.
5. Develop and institute preventive measures to prevent or reduce hazards and threats.
6. Identify and determine critical control points for your operation. These could be in general; locations, processes, functions, or time duration when your operation is at greatest risk, but in this paper it will be related also to preparedness of the specialists employees and functionality of the computers or other electronic systems and devices including the software used, e-mails received and if they are coming from free Internet e-mail services available to anyone in the world.
7. Establish and develop preventive or risk control measures to reduce hazards acceptable levels; these measures must include the insidious electronic hazards on controlling cyberspace too.
8. Establish critical limits (CLs) for the determined (CCPs). A particular CCP in this case could be related for example to some of these situations (each organization has got it's own specific situation):
  - The inquiry conditions or any other segments in your electronic controlling system.
  - The shortest time period before checking the functionality of the computers or systems or
  - Checking the ordered quantity of some chemicals which should be inquired in an acceptable limits in accordance to already established written procedures and whether the e-mail are not signed and contains for example inquiry about long-term storage of highly toxic pesticide in two-liter soft-drink-type bottles (6)
9. Establish or Develop monitoring procedures for each CCP. Monitoring is a systematic periodic activity to ensure that critical controls are in place and have not been breached or compromised in any way. These should be in writing. Make sure your monitoring procedure works and is both tolerable and feasible for your organization. Passwords and IDs validity for the other departments or the validation of some codes or signatures of people involved in the Cyberspace used in a whole.
10. Establish and Develop a procedure as a corrective action program under HACCP to fix electronic security problems or failures that occur if a critical control has been breached or compromised.
11. Ensure that electronic security problems are fixed. Revise critical controls and/or monitoring procedures accordingly. Retest monitoring procedures. The nature of some suspicious inquiries and of the specific highly toxic chemicals for instance, have to cause the specialist to forward the above mentioned e-mail concerning the long-term storage of highly toxic pesticide to the management in his organization or perhaps directly to the authorities. A special report related must be prepared too.
12. Establishing a Verification of the System; Test or verify periodically the developed security program to ensure that it works properly.
13. At the end, establish effective record keeping for the HACCP system in your company. This would include records of hazards and their control methods, the monitoring of safety requirements and action taken to correct potential problems. Having a confidential (Excel) written protocol is vital; it should be revised as your operations, electronic system, machines or equipments change.

The success of HACCP program is every ones responsibility and dependant also on its correct implementing during every production run. We all must work together toward a common goal of making sure that our food and water supplies everywhere in the world are fully safe and controlled by safe cyberspace.

## CONCLUSION

While the perpetrators of cyber-crime can carry out their activities in this apparently seamless environment, law enforcement is constrained by issues of jurisdiction. However, assessing the real extent of the future threat from cyber-terrorism requires conceptually clear strategic analysis and more detailed case studies and related training courses prepared by HACCP specialist, food safety scientists, research workers, electronic infrastructure experts and computer security advisors.

If the computer security advisor at your organization states that your Cyberspace related to your food processing chain is safe behind a system put into place by people who have never heard about "cyber-battles", behind firewalls,

behind audit trails, passwords, and encryption or other possibilities, then be sure that a great and dangerous fallacy is being perpetrated upon your food establishment or organization.

The key to preventing from terrorist attacks on your Cyberspace is coming from improving quality control and implementing a reasonable security measures at production facilities based on vulnerability assessment.

Rooted in the above context, this paper sets out a novel method for defeating cyber-terrorism's threats by implementing the enhanced HACCP Based Defeating Plan against possible terrorist threats to food & water supplies aimed at crippling the Cyberspace of the sophisticated food chain. Improving the preparedness and robustness of our Cyber security defenses continually evolves as the technology develops and thus this policy must ensure that continually collaborate and work together to ensure that our Cyberspace is secure by implementing correctly the enhanced security plan based on HACCP principles as described above.

On the other hand, highly trained HACCP team with its enhanced structure in today's operational environment will show that only knowledge management using secure information communication technologies can ensure that we can realistically aspire and achieve our local and global collective vision.

Authors of this paper suggest that all governments have to improve communications among themselves and with other governmental organizations involved in intelligence and response to food terrorism. On the other hand, communication and cooperation with industry is also critical. Governments must have written procedures of basic controlling systems to prevent deliberate contamination of their food supplies and, if threaten or attacked, to respond rapidly to minimize efficiently the health, economic and other effects (7). Food industry representatives should report all possible or actual threats of terrorism to their local authorities or to the government. Sometimes people are reluctant to contact local authorities, but this is truly a case where we, all over the world, must pool our intelligence resources and work together to save our food and water recourses. Finally, Cooperation between governments in all countries has to occur and exchanging information is something vital in order to minimize threat and contamination to critical infrastructures or areas of vulnerability such as agriculture & food and water supplies.

## REFERENCES

1. Computer Science and Telecommunications Board (CSTB), National Research Council. 1991. *Computers At Risk: Safe Computing in the Information Age*. National Academy Press, Washington, D.C.
2. David L. Carter (2003). *Computer crime and cyber terrorism, an overview*. School of Criminal Justice, 560 Baker Hall, Michigan State University, East Lansing, MI 48824-1116.
3. Mohamad Azzam Sekheta, Abeer H. Sahtout, Nizam F. Sekheta, Medhija Kapkovic and Nela Pantovic (2005). *The HACCP Implementation and the Mental Illness of Food Handlers as the 4th Eventual Hazard*. *Internet Journal of Food Safety*. Vol. 6, pp 5-10.
4. Papo-Griffin (2001). *Terrorism on the Hoof: Livestock as a Bioterrorism Target*. *Agrichemical & Environmental News*. No. 187.
5. U.S. Food and Drug Administration (1997). *Hazard analysis critical control point principles and application guidelines*. U.S. Department of Agriculture National Advisory Committee on Microbiological Criteria for Foods Adopted.
6. Carol Ramsay and Catherine Daniels (2001). *Pesticides as Weapons. Agrichemical Industry's Role in Anti-Terrorism*. *Agrichemical and Environmental News*, No. 187.
7. Stefano Baldi, Eduardo Gelbstein, and Jovan Kurbalija *Hackivism* (2003). *Cyber-terrorism and cyberwar*, ISBN 9993253049, Diplo Foundation.