Ecology of Spam Server Under Resilience Force in the e-Network Framework

Katsuko T. Nakahira, Kakeru Yamaguchi, and Muneo Kitajima

Nagaoka University of Technology
Niigata, Japan
Email:katsuko@vos.nagaokaut.ac.jp,yukidaruma1232@yahoo.co.jp,mkitajima@kjs.nagaokaut.ac.jp

***Abstract*—We propose the concept "*ecology of a spam server*," based on the *e*-Network and *resilience* in an effort to clarify its mechanism, which will contribute to the development of security and network strategies. We consider the microstructure of *resilience* with the *e*-Network framework and demonstrate three stages of spam servers: secure but underlying, developing, and critical. Using these features, we introduce the Evolution Diagram (ED), a method for quantitatively representing the patterns of the evolution history of a server. From this diagram, we derive three indexes to measure resilience: maximum transmission potential, continuity, and reproducibility. Through these indexes, we define resilience, which is divided into eight classes depending on the existence/absence of these three primitive features. We calculate the *resilience* of the individual spam servers. This idea would lead to useful tools for producing strategies not only for security but also for Internet/country domain governance.**

Keywords–ecology of spam server, resilience, e-Network, ED transition diagram

I. INTRODUCTION

In this study, we develop the concept "ecology of a spam server" in an effort to understand the mechanism under which spam evolves and spreads. In addition, we determine how it is related to the *e-Network* [1].

Currently, spam is considered a principal factor that may cause serious problems (e.g., decreasing one's productivity due to the slip of important mail and increasing the cost of administrating mail substratum). Many studies have been conducted and a number of white papers have been published concerning security-related spam. These studies have proposed a variety of anti-spam strategies. For example, Graham [2] addressed the following issues based on the userprovider configuration and networking scheme with some descriptions of advantages, demerits, and roles of various categories: filtering (signature-based/Bayesian (statistical) rule-based (heuristic)/challenge-response), secret address, junk address, penny per mail, mail server blacklists, filters that fight back (FFBs), slow senders, laws, and complaints to spammers' Internet Service Provider (ISP)'s. Recently, other strategies have been developed. Li and Hsieh [3] developed a group-based anti-spam framework. They analyzed community behavior of spammers through a large collection of spam mail to identify structures of spammers using spam traffic data collected on a domain mail server. They suggested that the number of members in a group and the number of groups with which a spammer is associated are useful measures for developing group-based anti-spam strategies. Stanković and Simič [4] proposed effective strategies for defending against botnets, consisting of a list of measures and activities along with some explanatory descriptions. Van Staden and Venter [5] proposed anti-spam strategies for detecting botnet activities and tracing botmasters.

Expanding this research, the objective of the present study is to construct a method for estimating Internet governance for each region in the world. To do this, we assume that the spam server exists as social ecology. Thus, we must understand spam servers' behavior in the context of *human* involvement. In this paper, we introduce two concepts, the *e*-Network and *resilience*, to clarify the *ecology of* a spam server. By definition, spam servers distribute spam mail. However, the spam server is not installed as a "spam server" from the outset. It "behaves" as a spam server at the moment but may return to acting as a "normal" server at any time in the future. However, it may continue to behave as a spam server, or even become a worse spam server. How the behavior of a spam server changes over time depends on several technological, human, and social factors. This study regards this phenomenon as the ecology of a spam server. This paper discusses dynamics in the *e*-Network framework [1] and proposes *resilience* as a primary force that shapes the behavior of spam servers.

e-Network. This study assumes that the ecology of a spam server should emerge from interactions among the factors defined in the *e*-Network framework proposed by [1]. Table I lists the fundamental components in the *e*-Network: human factor, substratum factor, products factor, and environment factor. The media, which are restricted to spam mail in this study, connect them. The following are examples of interaction between factors:

- A user who intends to send spam mail must use PCs and ISPs (human-substratum interaction).
- A user sends spam mail to earn money (human-environment interaction).
- The registry must control Top Level Domain (TLD)s (substratum-environment interaction).

Resilience force. *Resilience*is defined as "the ability of a network administer and maintain an acceptable level of service in the presence of various faults and [such] challenges to normal operations" in the context of network risk management, focusing on the relationship between security and *resilience* (e.g., see [6] and [7]). This study, however, reinterprets it within the *e*-Network framework: a server that has become a spam server might revert to a normal secure server as a result of interactions between the substratum factor (server and network) and the

 ISBN: 978-1-61208-390-2

TABLE I. THE FRAMEWORK COMPONENTS IN E-NETWORK

component	role	variable
human factor	*human behavior*	user
substratum factor	*the device for execution*	client, server, the Internet
environment factor	*surround human and substratum*	law, freedom of speech, education, income, a custom, etc.
product	*produced from interaction with human and substratum factor*	information contents
media	*connection device between the relation of all components*	language, images, etc.

human factor, environment factor, and/or products factor. Some interactions could be strong enough to make an insecure server revert to a secure one, whereas others could be too weak to make this happen. This paper metaphorically considers that these interactions work as a source of forces, called *resilience* force here.

Resilience force characterizes the state of a spam server over time. It could be secure, developing, or critical. If the *resilience* force of a server is strong, it allows the server to revert to its secure state even if the server begins sending spam mail. If the *resilience* force of a server is weak, a server that has begun to send spam mail is likely to develop the spam-sending activity to a critical state.

In the following sections, this paper regards the phenomenon that a spam server changes its state over time as the evolution of a spam server, and proposes the *Evolution Diagram (ED)* for quantitatively representing the pattern of a spam server's evolution. An ED value, which is a cumulative and integral value characterizing the evolution history of a server, and its derivatives (e.g., reproducibility, continuity, and potential) are candidates for expressing how *resilience* force has worked on the server. In section 2, we introduce three ecological stage of a server in the *e*-Network. In section 3, we develop the method how to measure strengths of *resilience* force with ED. In section 4, we construct ED transition diagram and relate to *resilience*. In section 5, we discuss two ecological scenarios for spam server. In section 6, we show the results of observed ecology for spam servers.

II. THREE ECOLOGICAL STAGES OF A SERVER IN THE *e*-NETWORK

A server can be in one of the three ecological stages in the e-Network: secure but underlying, developing, or critical. Each of these stages is closely related to how the *resilience* force works in the situation defined by the detailed conditions of the *e*-Network around the server. Using Fig. 1, this section explains the conditions of the elements of the *e*-Network (human (users), substratum, and environment (government)) and their interactions, and introduces *resilience* force.

Stage 1: Secure but underlying. When a mail server installs or starts mail service, it should be secure. However, it could become a spam server just because it works as a mail server. Therefore, the status of a mail server at this stage is "secure and underlying" for several reasons. It is likely that a new mail server is equipped with the latest versions of OS and protocol. In addition, when a mail service is started, most users who want to use this service are moral users. The scale of service is just right for skilled administrators to run and maintain it appropriately. The range of mail usage is limited: users use the service simply to contact their friends, family, or business partners. They tend to reject its immoral use. For these reasons, Internet governance is maintained by the behavior of moral users.

Moving to the underlying state. As time goes by, the conditions that allow the server to keep its status secure may change, and some problems may arise. The first spam is generated. However, this process occurs only occasionally. For example, immoral users who join the service may send illegal spam e-mail (e.g., junk mail). In order to deal with the increased number of users, the service provider must reinforce the server's substratum (e.g., deploy new servers or increase transmission speed). As the number of servers grows and the transmission rate increases, the administrator's task of keeping the service secure becomes more complicated. Due to the shift of service users' and providers' structures, some mail servers may allow a large amount of junk e-mail to be sent, mainly because the administrator cannot distinguish good e-mail from junk e-mail.

Staying in the secure and underlying state. With strong *resilience* force, the service provider can stay in the secure but underlying state by reducing the possibility of immoral use through broadcast constraints, enhanced maintenance, and skilled administrators.

Moving to the developing state. With weak *resilience* force, a server moves to the developing stage, where it sends spam mail chronically. This stage is triggered by worsening behavior of users and/or the substratum. Some users may become involved in immoral behavior, such as developing immoral technology (e.g., virus software), hacking/cracking algorithms, and automatically sending spam programs. The server provides little maintenance, due to the lack of skilled administrators and a poor engineering staff.

Stage 2: Developing. A strong *resilience* force originating from the social system might produce several strategies to improve the service server conditions and cause it to revert to the secure and underlying stage. Otherwise, the number of immoral service users will increase, and immoral technologies will proliferate continuously and widely.

A strong *resilience* force originating from Internet governance results in increased control over these immoral behaviors through laws or strict governance. These interventions involve legal force to punish these immoral behaviors. Through these strategies, most users and service providers avoid such spam behavior and obey the law. The servers that are in the "developing" stage will revert to the "secure and underlying" stage. Otherwise, the server may move to an even worse stage, the critical stage.

Stage 3: Critical. With ultra-weak *resilience* or no *resilience*, the server stays in the critical stage. Here, immoral behavior and the use of immoral technology may reach the pandemic level, and service providers cannot control their service quality. Internet governance cannot control these conditions.

 ISBN: 978-1-61208-390-2

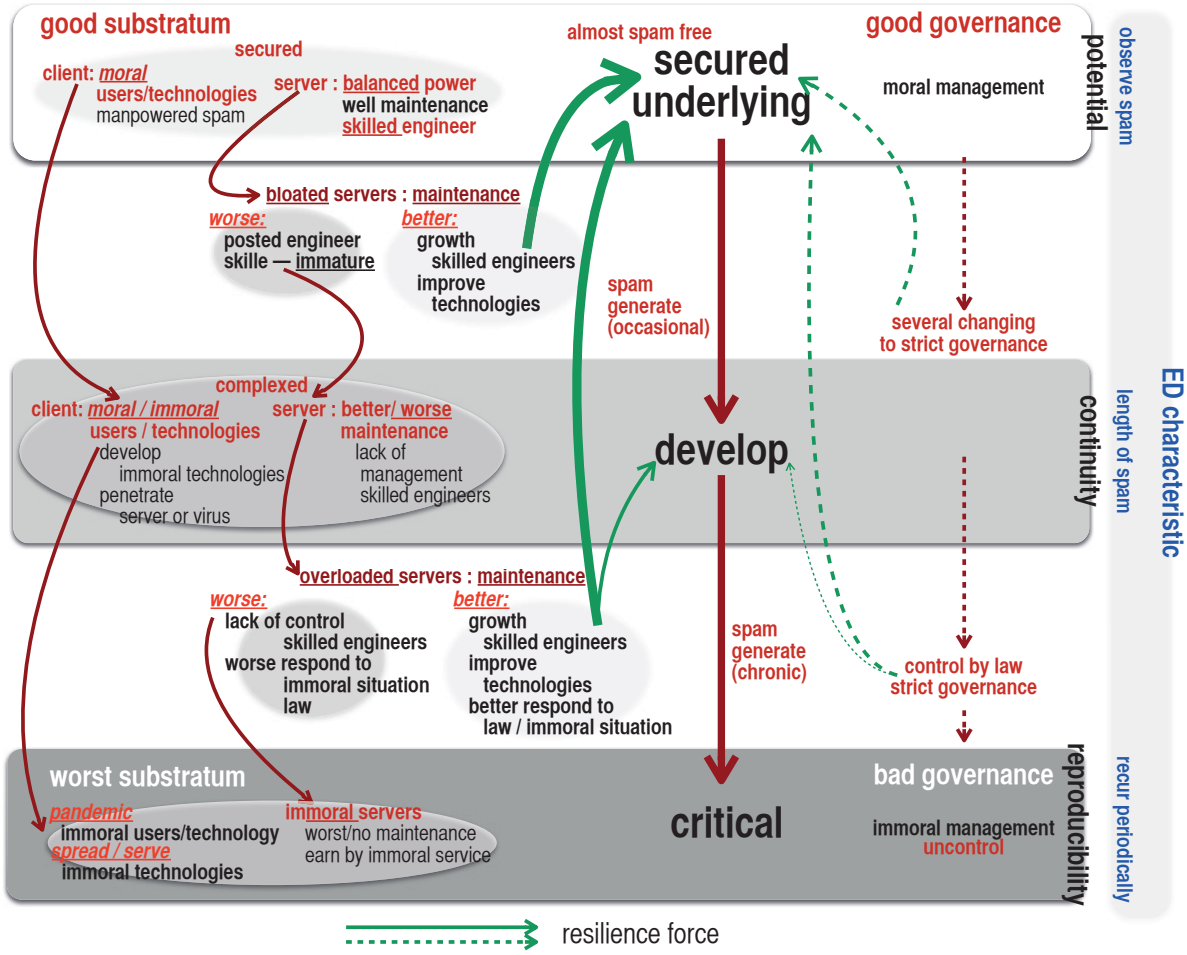

Figure 1. Microstructure for resilience.

III. Evolution Diagram and Its Derivatives for Measuring Strengths of Resilience Force

A. Evolution Diagram (ED)

An Evolution Diagram (ED) is a method of quantitatively representing the pattern of evolution history concerning a particular event (e.g., sending spam mail). For a given duration of observation of an event, (e.g., 1 year), we obtain a series of event-occurrence times as the data. We are interested in the tendency of change in the density of event occurrences over time, which should be related to the *resilience* force of the agent, (i.e., the spam server) that generates the event. An effective method of characterizing it is to analyze the data with different time resolutions (e.g., 1 year, 1/2 year, 1/4 year, and 1/8 year) and record "observed" if there is an event occurs in the time range or "not-observed" if there is none. Let the minimum observation time for detecting spam mail be τ (typically τ = 1sec), and the total observation time be T, which is a multiple of τ. By assigning "1" if an event is observed and "0" if none is observed, we can generate a series of 1s and 0s with the length of T/τ, denoted as $\vec{a} = (a_1, \cdots, a_{T/\tau})$.

In order to analyze the event-occurrence series in a variety of time resolutions with an arbitrary observation time unit, $\delta t = j \times \tau$, where $j = 1, \cdots, T/\tau$, we create $\vec{b}^{(j)} = (b_1, \cdots, b_i, \cdots, b_{L^{(j)}})$ from $\vec{a}$, where $L^{(j)}$ is the partition number calculated by the following formula:

$$L^{(j)} = \lfloor \frac{T}{j \times \tau} \rfloor. \quad (1)$$

In here, any positive integers in the range are allowed, but we use $j = 1, 2, 4, \cdots, 2^n (= T)$ for the sake of brevity of calculation.

The most coarse observation corresponds to $L^{T/\tau} = 1$, and the most precise observation corresponds to $L^{(1)} = T/\tau$. Here, $\vec{b}^{(j)}$ represents a seriese of event occurrences for the given time resolution $\delta t = j \times \tau$, as a series of 1s and 0s; $b_j = 1$ if the event is observed during the i-th observation period with the time resolution of δt, or 0 if non is observed. The ED value, $I(j)$, is calculated from $\vec{b}^{(j)}$ by applying the following formula:

$$I(j) = \sum_{i=1}^{L^{(j)}} b_i^{(j)} / L^{(j)}, \quad (2)$$

where $I(j)$ has value between 0 and 1.

An ED is created by plotting ED values as a function of j, where $j = 1, \cdots, T/\tau$, which is actually used to calculate

 ISBN: 978-1-61208-390-2

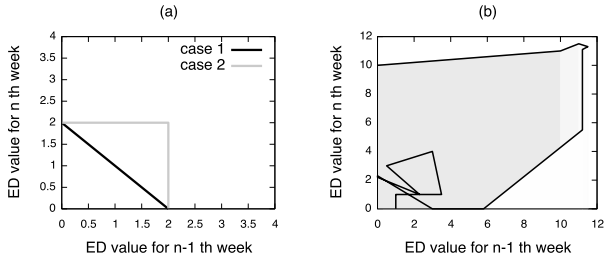

Figure 2. (a) Example of ED transition. (b) Example of calculation of Continuity and Reproducibility.

TABLE II. ED-VALUES IN THE CASE OF $T = 1$, TOTAL NUMBERS OF SPAMS ARE IN THE PARENTHESIS

Number of spams per 1 month		1 spam	5 spams	10 spams	30 spams
1 month		2.00 (1)	2.25 (5)	2.34 (10)	2.48 (30)
continue	2 months	2.13 (2)	2.99 (10)	3.17 (20)	3.45 (60)
	3 months	2.63 (3)	3.41 (15)	3.70 (30)	4.10 (60)
	4 months	2.88 (4)	3.72 (20)	4.06 (40)	5.57 (120)
equal interval	6 months	3.00 (2)	3.99 (10)	4.16 (20)	4.42 (60)
	4 months	3.50 (3)	4.37 (15)	4.64 (30)	5.06 (90)
	3 months	4.00 (4)	4.99 (20)	5.57 (40)	6.34 (120)

the ED values. ED values increase monotonically to 1 as j approaches its maximum value, T/τ, if if the server has sent at least one spam mail during the observation period.

The total ED value for the k-th observation series is calculated by summing the ED values for the actually taken j values:

$$\mathrm{ED}(k) = \sum_{j=\{1,\cdots,T/\tau\}} I(j). \tag{3}$$

B. Relationship between total ED values and Spam Sending Patterns: Simulation

Table II presents the results of the calculation of total ED values for artificially generated spam-sending patterns. The length of observation T is set to $T = 2^{24}$ sec, which is 194 days or 6.5 months, and $j = 2^0, 2^1, 2^2, 2^3, \cdots, 2^{24}$. The columns represent four different spam-sending patterns in terms of the total number of spams (1, 5, 10 and 30). It is assumed that spam-sending events occur periodically. For example, when the total number of spams is 10, one spam is sent every 3 days. The rows indicate the length of seven spam-sending patterns: 2, 3 or 6 months, and recurring patterns with 6-, 4-, and 3-month intervals. The figures in parentheses indicate the total number of spams sent in a year in the 28 different spam-sending conditions, for referencing purposes.

The total ED values are not necessarily proportional to the total number of spams. Comparison of the four cases where the total number of spams per year is 20 indicates that "5 spams/month with the equal interval of 3 months (i.e., 5, 0, 0, 5, 0, 0, $\cdots$)" has the worst total ED value (4.99). The case "10 spams/month lasting 2 months (i.e., 10, 10, 0, 0, 0, 0, $\cdots$)" has the lowest total ED value (3.17). The cases "5 spams/month lasting 4 months (i.e., 5, 5, 5, 5, 0, 0, $\cdots$)" with the total ED value of 3.72 and "10 spams/month with the equal interval of 6 months (i.e., 10, 0, 0, 0, 0, 10, 0, $\cdots$)" with the total ED value of 4.16 are in-between.

IV. RESILIENCE AND ED TRANSITION DIAGRAM

A. ED Transition Diagram

Introducing *resilience*, we can mark spam servers' states or degrees of healthiness. We derive *resilience* using an ED transition diagram as explained below. An ED transition diagram is defined on an $x-y$ plane. Each point has $(n-1)$-th total ED value as the x value and n-th total ED value as the y value. Combining the points for $n = 1, \cdots$, we can draw a figure with connected lines. In the following example, we calculate total ED values by setting $T = 2^{20}$, approximately 12 days. If $(n-1)$-th and n-th week's total ED values are different, we judge that there have been some changes in conditions.

Figure 2 (a) presents ED transition diagrams for two ideal cases. N is set to 20, with 1 week of observation time. In case 1's simulation, spam is detected only once every 6 months; the ED value is 2 when spam is detected and 0 when no spam is detected. Therefore, the coordinates change in the order (0, 0) $\rightarrow$ (0, 2) $\rightarrow$ (2, 0), and a corresponding triangle appears. In case 2's simulation, spam is detected every week. The coordinates change in the order (0, 0) $\rightarrow$ (0, 2) $\rightarrow$ (2, 2) $\rightarrow$ (2, 0), and a corresponding square appears. These two examples demonstrate that if the same ED value is calculated from different event occurrence patterns, different closed trajectories are obtained. Using these features, we define three elements for *resilience*: maximum transmission potential, continuity, and reproducibility.

Maximum transmission potential. The maximum transmission potential of *resilience* is determined from the area of the outer edge in the ED transition diagram. It is calculated by the area of a closed surface. In the example depicted in Fig. 2 (b), the gray zone is the value of maximum transmission potential. The outer edge of the ED transition diagram indicates the most active spam transmitting in the period. The area depends on the amount of spam transmission and the frequency for the most malicious condition of the server.

Continuity. Continuity represents the line integral of the ED transition diagram's trajectory. Practically, we calculate the Euclidean distances along the trajectory. The total distance depends on the duration of spam-sending.

Reproducibility. Lastly, we characterize spam transmission patterns by taking into account the direction of line segments that constitute the ED transition diagram. Here, we define six codes for y_n as week n's ED value:

- `S` : $y_{n-1} = 0,\ y_n = a$,
- `G` : $y_{n-1} = a,\ y_n = 0$,
- `_` : $y_{n-1} = a,\ y_n = a$,
- `E` : $y_{n-1} = 0,\ y_n = 0$ (repetition of `E` is counted as a single `E`),
- `U` : $y_{n-1} = a_1,\ y_n = a_2\ (a_1 < a_2)$,
- `D` : $y_{n-1} = a_2,\ y_n = a_1$.

For example, Fig. 2 (a) represents as `ESGE`, and Fig. 2 (b) represents as `ES_UGS`$\cdots$`GE`. In cases, Fig. 2 (a) has single `S` and (b) has several `S`, which means condition (b) is worse index value of reproducibility. Following these codes, reproducibility can be defined as the number of `S`.

 ISBN: 978-1-61208-390-2

TABLE III. CLASSIFICATION OF RESILIENCE FORCE, CHECKS ARE GIVEN FOR MALICIOUS COMPONENTS

class No.	reproducibility (R)	continuity (C)	potential (P)
0			
1(P)			√
2(C)		√	
3(CP)		√	√
4(R)	√		
5(RP)	√		√
6(RC)	√	√	
7(RCP)	√	√	√

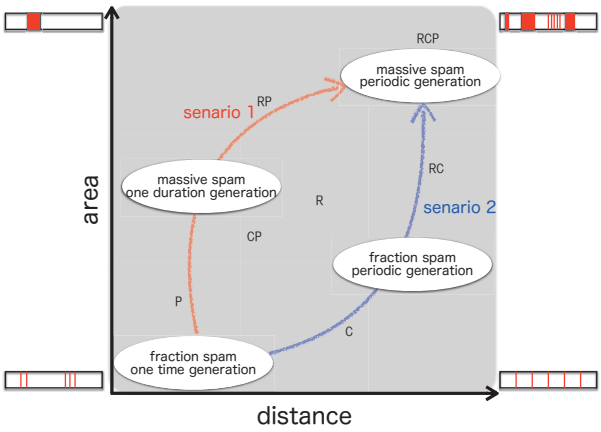

Figure 3. Relation of 2 senarios for spam server ecology and *resilience* class.

B. Resilience classes

Finally, we determine *resilience* for spam servers based on three components: maximum transmission potential, continuity, and reproducibility. We set the threshold value of the components to the values of the top 75% of these elements, and estimated the normalized degree of *resilience* of each server. Here, the normalization factor was the value for a server that sent spam mail once during the period.

Table III lists the *resilience* classes defined by counting the components whose values exceed the threshold values.

Most servers are classified as class 0. The ratios of No. 6 (CR), No. 1 (P), and No. 7 (PCR) are higher. Hence, No. 6 (RC) is server to send a long period of time a small amount of spam, No. 1 (P) is server to send a short period of time a large amount of spam, No. 7 (RCP) is server to send a long period of time a large amount of spam elements of the *resilience* has a meaning separate. Each component of *resilience* has a different meaning. Reproducibility R and continuity C mean weakness of *resilience*. Reproducibility is a measure of server status change and turbulence of ED value, and continuity is strongly related to the reproducibility cause of generating a line integral of ED transition. Hence, higher reproducibility and continuity indicate weak *resilience*. Maximum transmission potential is a useful component for measuring the strength of *resilience* in contrast with continuity and reproducibility. Even though maximum transmission potential is large whereas continuity and reproducibility are low, better control and management of servers derive low continuity and reproducibility. In a sense, maximum transmission potential functions with the combination of continuity and reproducibility.

V. TWO ECOLOGICAL SCENARIOS FOR SPAM SERVER

Using these analyses and simulations, we develop the "ecology of a spam server." Evans [8] summarized two distinct cognitive systems underlying reasoning: system 1, which is rapid, parallel, and automatic in nature; and system 2, which involves abstract hypothetical thinking. Coordinating these two systems, a human can make decisions. Applying this idea, we construct two ecological scenarios for a spam server (Fig. 3). First, we set two parameters, distance and area, in the ED transition diagram. Distance represents continuity with periodic spam-sending from the server. When a spam server tries to set the duration of a period, the server uses reasoning, such as safety (undetected by the administrator) duration. In this case, the distance is long but the area is small, as denoted by the line indicated as scenario 2 in Fig. 3. Area represents the maximum transmitting potential of the server. When a spam server tries to send many spam mails, it does not need to think about whether or not it has the potential to send so much mail. The only behavior of the server or spammer is sending spam without setting the duration of the period; it simply sends while the administrator does not stop the behavior. This behavior is denoted by the scenario 1 line in Fig. 3. Usually, System 2 monitors how System 1 behaves and warns System 1 when it captures System 1 attempts to send a lot of spam mails. Compared with Fig. 1, this stage is regarded as "secure but underlying." If system 1 or 2 arises in the server, the stage of the server will change to "developing." In this stage, if the *resilience* force is very strong, the server recovers its two systems' cooperation (i.e., the stage will return to "secure but underlying") . If the *resilience* force is weak, the server's two systems exhibit worse resonance: System 2 fails to warn System 1 not to send spam mails and as a consequence System 1 attempts to send spams more frequently in the shorter duration. The stage of the server will then be "critical" (upper right-hand area of Fig. 3). The stage of the server will then be "critical" (upper right-hand area of Fig. 3). Many resources are available to prevent changing to worse stages. One is security technology. In addition, human ability (e.g., administrators' management skills and users' morality) is also important. If human behavior does not change, the environment (e.g., Internet governance or regional management laws) must become stricter. Using analysis of spam servers' ecological features in the network's geological regions, we encourage regional management of the Internet. Finally, we observe features of the regional ecology of spam servers to provide several suggestions for management.

VI. OBSERVED ECOLOGY OF SPAM SERVERS

We collected "spam mail headers," which are the headers of mail identified as spam by mail-filtering software (SpamAssassin) at our university. Observation was conducted from March 1, 2013, through February 28, 2014. We identified 1,733,929 domains and 21,332,168 spam headers. For demonstration purposes, we randomly extracted 10,000 domains. The total ED value of each domain was calculated by setting $T = 1$ year and $j = 2^0, 2^1, 2^2, 2^3, \cdots, 2^{24}$. Note that the possible total ED values are limited. Only 5,703 domains have a total ED value of 2. As indicated in Table II, this value corresponds to the spam-sending pattern "one spam mail sent in a year." In addition, 2,109 domains have a total ED value of 2.5. Figure 4 plots the relationship between maximum transmitting potential and continuity for 10,000 spam domains, which are

 ISBN: 978-1-61208-390-2

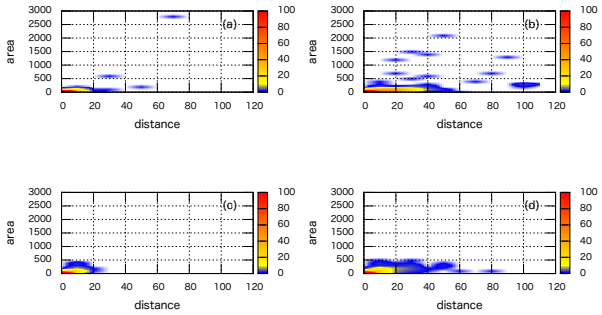

Figure 5. Sample of several stage at senario 1 and 2 for several ccTLD area. (a) senario 1 stage, (b) worst stage, (c) initial stage, (d) senario 2 stage.

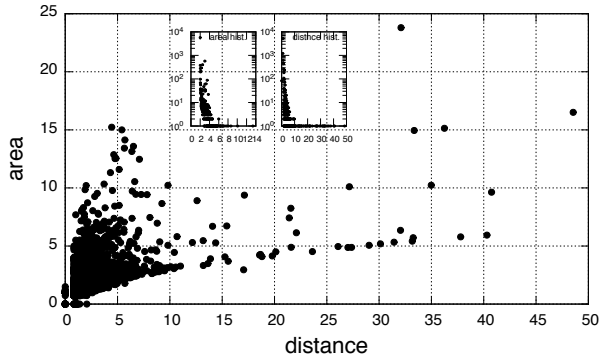

Figure 4. Relation of value of distance and area.

measured by the amount of outer area and line integral of ED transition diagram, respectively. for 10,000 spam domains. The graph depicts the distribution of each server's area (left side)/distance (right side). We find that the distribution of distancearea relationships exists between the four points in Fig. 3. Typically, large area and short distance are a healthy state for the transmission of spam in a short term (1 to 3 weeks). For this reason, the total ED value tends to become smaller. This class is equivalent to sending 30 spams in a month in Table II. Separating observed points in Fig. 4 from each geological server, we can determine the regional features of server management. In the graph, we show the histgram of area (left side)/distance (right side) value. Histgrams' horizontal axis represents normalized value of area/distance, and vertical axis represents the fraction of occurence. Figures 5 (a) through (d) present observed typical examples of the four geological regions' ecology of spam servers. The contour indicates the number of spam servers at the different values. We found four types of ecology derived from Fig. 3. For example, we regard (c) in Fig. 5 as "stable but underlying," (a) and (d) as "developing", and (b) as "critical." With the four features and microstructure in Fig. 1, we can estimate the network region's server management. Fig. 5 (a) represents that a number of servers are in the state of high continuity. In contrast, Fig. 5 (d) represents many servers are in the state of high reproducibility. Fig. 5 (b) shows a number of servers are in the state of high continuity or reproducibility. We can find these features in each ccTLD area. With the results, we can guess how the geological area's Regional/National Internet Registry makes Internet management policy: each Internet Registry has already had effective strategies for the Internet communication with specific reasons, or requires to enforce the area's Internet security of management.

VII. Conclusion

In this study, we proposed the concept "ecology of a spam server," based on the *e*-Network and *resilience* in an effort to understand the mechanism. First we considered the microstructure for *resilience* with the *e*-Network framework and demonstrated three stages for spam servers: secure but underlying, developing, and critical. Each stage included several features of potential/observe, continuity/length of spam, and reproducibility/periodic recurrence. Using these features, we introduced ED, a method for quantitatively representing the pattern of evolution history concerning a particular event, analyzing the data with different time resolutions and recording observed events. Using the ED values, we generated an ED transition diagram and defined three components to measure *resilience*: maximum transmission potential (calculated by area of closed surface), continuity (line integral for the ED transition diagram's trajectory), and reproducibility (number of restarts of spam emailing). Through these processes, we define eight classes of *resilience* with these three components and analyze tentative features of spam server behavior. Thus, we can advance the study of the ecology of a spam server, which will be a useful tool for producing strategies not only for security but also for the Internet/country domain governance.

Acknowledgment

The study described in this paper has been partially funded by the Scientific Research Expense Foundation C Representative: Katsuko T. Nakahira (24500308).

References

[1] K. T. Nakahira, "A Framework for Understanding Human e-Network – Interactions among Language, Governance, and more. " [Online]. Available: http://www.maayajo.org/IMG/SIMC/paris-v2.pdf[accessed2015-02-10]

[2] P. Graham, "Different Methods of Stopping Spam." [Online]. Available: http://www.windowsecurity.com/whitepapers/anti_spam/Stopping_Spam.html[accessed2014-09-10]

[3] F. Li and M. han Hsieh, "An Empirical Study of Clustering Behavior of Spammers and Groupbased Anti-Spam Strategies," in CEAS 2006 Third Conference on Email and AntiSpam, 2006, pp. 27–28.

[4] S. Stanković and D. Simič, "Defense Strategies Against Modern Botnets," CoRR, vol. abs/0906.3768, 2009. [Online]. Available: http://arxiv.org/abs/0906.3768

[5] F. V. Staden and H. S. Venter, "The State of the Art of Spam and Anti-Spam Strategies and a Possible Solution using Digital Forensics." in ISSA, H. S. Venter, M. Coetzee, and L. Labuschagne, Eds. ISSA, Pretoria, South Africa, 2009, pp. 437–454. [Online]. Available: http://www.bibsonomy.org/bibtex/2a914634f9302a8e9b54425ab149e0e5d/dblp[accessed2015-02-10]

[6] P. Smith, D. Hutchison, J. P. Sterbenz, M. Schöller, A. Fessi, M. Karaliopoulos, C. Lac, and B. Plattner, "Network Resilience: A Systematic Approach," IEEE Communications Magazine, vol. 49, no. 7, July 2011, pp. 88–97.

[7] "Measurement Frameworks and Metrics for Resilient Networks and Services: Technical Report," European Network and Information Security Agency, Tech. Rep., Feb. 2011.

[8] J. S. B. T. Evans, "In two minds: dual-process accounts of reasoning," Trends in Cognitive Sciences, vol. 7, no. 10, 2014/11/15, pp. 454–459. [Online]. Available: http://www.cell.com/trends/cognitive-sciences/abstract/S1364-6613(03)00225-0[accessed2015-02-10]

 ISBN: 978-1-61208-390-2