

spatial coverage of measures of soil loss). Third, an expanded set of ecosystem services could be quantified, including ecosystem contributions to securing water and air quality, both of which have deteriorated in China in recent decades, and mental health benefits of exposure to nature (24). Fourth, improved measures can be used that more directly link ecosystem services to human well-being, such as economic measures of value and direct measures of impact on health, livelihoods, happiness, or other aspects of well-being (25, 26). Finally, better understanding of human behavioral responses to changes in policy or market conditions could improve policy effectiveness. Regularly repeating the CEA can provide insight into future national development pathways (27).

REFERENCES AND NOTES

- Q. Ye, M. H. Glantz, *Mitig. Adapt. Strategies Glob. Change* **10**, 159–182 (2005).
- J. Liu, S. Li, Z. Ouyang, C. Tam, X. Chen, *Proc. Natl. Acad. Sci. U.S.A.* **105**, 9477–9482 (2008).
- P. Zhang *et al.*, *Science* **288**, 2135–2136 (2000).
- J. Liu, Z. Ouyang, W. Yang, W. Xu, S. Li, in *Encyclopedia of Biodiversity*, S. A. Levin, Ed. (Academic Press, Waltham, MA, ed. 2, 2013), pp. 372–384.
- M.-N. Tuanmu *et al.*, *Conserv. Biol.*, 10.1111/cobi.12669 (2016).
- Materials and methods are available as supplementary materials on Science Online.
- R. Sharp *et al.*, *InVEST +VERSION+ User's Guide* (The Natural Capital Project, Stanford University, University of Minnesota, The Nature Conservancy, and World Wildlife Fund, 2015).
- P. Kareiva, H. Tallis, T. H. Ricketts, G. C. Daily, S. Polasky, Eds., *Natural Capital: Theory and Practice of Mapping Ecosystem Services* (Oxford Univ Press, New York, 2011).
- I. J. Bateman *et al.*, *Science* **341**, 45–50 (2013).
- J. J. Lawler *et al.*, *Proc. Natl. Acad. Sci. U.S.A.* **111**, 7492–7497 (2014).
- S. Hatfield-Dodds *et al.*, *Nature* **527**, 49–53 (2015).
- Millennium Ecosystem Assessment, *Ecosystems and Human Well-Being: Synthesis* (Island Press, Washington, DC, 2005).
- UKNEA (UK National Ecosystem Assessment), *The UK National Ecosystem Assessment Technical Report* [United Nations Environment Programme (UNEP)–World Conservation Monitoring Centre, Cambridge, 2011].
- UNEP, Intergovernmental Science-Policy Platform on Biodiversity and Ecosystem Services, Decision IPBES-2/4: Conceptual framework for the Intergovernmental Science-Policy Platform on Biodiversity and Ecosystem Services: Report of the second session of the plenary of the Intergovernmental Science-Policy Platform on Biodiversity and Ecosystem Services (UNEP, 2014).
- WAVES (Wealth Accounting and the Valuation of Ecosystem Services), *WAVES Annual Report 2015* (World Bank, Washington, DC, 2015).
- P. R. Ehrlich, P. M. Kareiva, G. C. Daily, *Nature* **486**, 68–73 (2012).
- Ministry of Environmental Protection of China and Chinese Academy of Sciences, *National Ecosystem Service Zoning in China* (Ministry of Environmental Protection and CAS, Beijing, 2015).
- Ministry of Environmental Protection, *National Ecological Protection Redlining* (Ministry of Environmental Protection, Beijing, 2015).
- China Council for International Cooperation on Environment and Development, *Report on Institutional Innovation of Ecological Protection Redlining* (CCICED, Beijing, 2014).
- Ministry of Transport of China, *National Road Development Planning (2014–2030)* (MTC, Beijing, 2013).
- A. Viña, W. McConnell, H. B. Yang, Z. C. Xu, J. G. Liu, *Sci. Adv.* **2**, e1500965 (2016).
- B. Fu, *Science* **321**, 611 (2008).
- J. G. Liu, P. H. Raven, *Crit. Rev. Environ. Sci. Technol.* **40**, 823–851 (2010).
- G. N. Bratman, J. P. Hamilton, G. C. Daily, *Ann. N.Y. Acad. Sci.* **1249**, 118–136 (2012).
- S. R. Carpenter *et al.*, *Proc. Natl. Acad. Sci. U.S.A.* **106**, 1305–1312 (2009).
- C. Folke, S. R. Carpenter, B. Walker, M. Scheffer, *Ecol. Soc.* **15**, 20 (2010).
- National Development and Reform Commission of China, *Opinions on Accelerating the Construction of Ecological Civilization* (NDRCC, Beijing, 2013).

ACKNOWLEDGMENTS

We thank the Ministry of Environmental Protection (MEP) of China and Chinese Academy of Sciences (CAS) for organizing the Project, and experts in 31 provinces for collecting the field data for statistics analysis on this manuscript. This work was supported by the Ministry of Finance of China through the

MEP/CAS project “Survey and Assessment of National Ecosystem Changes Between 2000 and 2010, China” and by the international Natural Capital Project. All the data are available at www.sciencedb.cn/dataSet/handle/73.

SUPPLEMENTARY MATERIALS

www.sciencemag.org/content/352/6292/1455/suppl/DC1
Materials and Methods
Figs. S1 to S5
Tables S1 to S5
References (28–98)

10 January 2016; accepted 18 May 2016
10.1126/science.aaf2295

HUMAN BEHAVIOR

New online ecology of adversarial aggregates: ISIS and beyond

N. F. Johnson,¹ M. Zheng,¹ Y. Vorobyeva,² A. Gabriel,¹ H. Qi,¹ N. Velasquez,² P. Manrique,¹ D. Johnson,³ E. Restrepo,⁴ C. Song,¹ S. Wuchty^{5,6*}

Support for an extremist entity such as Islamic State (ISIS) somehow manages to survive globally online despite considerable external pressure and may ultimately inspire acts by individuals having no history of extremism, membership in a terrorist faction, or direct links to leadership. Examining longitudinal records of online activity, we uncovered an ecology evolving on a daily time scale that drives online support, and we provide a mathematical theory that describes it. The ecology features self-organized aggregates (ad hoc groups formed via linkage to a Facebook page or analog) that proliferate preceding the onset of recent real-world campaigns and adopt novel adaptive mechanisms to enhance their survival. One of the predictions is that development of large, potentially potent pro-ISIS aggregates can be thwarted by targeting smaller ones.

Extremist entities such as ISIS (known as Islamic State) stand to benefit from the global reach and speed of the Internet for propaganda and recruiting purposes in ways that were unthinkable for their predecessors (1–10). This increased connectivity not only may facilitate the formation of real-world organized groups that subsequently carry out violent attacks (e.g., the ISIS-directed attacks in Paris in November 2015) but also may inspire self-radicalized actors with no known history of extremism or links to extremist leadership to operate without actually belonging to a group (e.g., the ISIS-inspired attack in San Bernardino in December 2015) (11). Recent research has used records of attacks to help elucidate group structure in past organizations for which the Internet was not a key component (3, 6, 12), the nature of attacks by lone-wolf actors (13), and the relationship between general online buzz and real-world events (14–16). Online buzz created

by individuals that casually mention ISIS or protests is insufficient to identify any long-term buildup ahead of sudden real-world events (see, for example, fig. S1). This leaves open the question of how support for an entity like ISIS develops online—possibly before any real-world group has been formed or any real-world attack has been perpetrated—whether by “recruits” or by those simply “inspired.”

Our data sets consist of detailed second-by-second longitudinal records of online support activity for ISIS from its 2014 development onward and, for comparison, online civil protestors across multiple countries within the past 3 years, following the U.S. Open Source Indicator (OSI) project (14–16). The supplementary materials (SM) provide a roadmap for the paper, data descriptions, and downloads. The data show that operational pro-ISIS and protest narratives develop through self-organized online aggregates, each of which is an ad hoc group of followers of an online page created through Facebook or its global equivalents, such as ВКонтакте (VKontakte) at <http://vk.com/> (Fig. 1). These generic web-based interfaces allow such aggregates to form in a language-agnostic way and with freely chosen names that help attract followers without publicizing their members’ identities. Because the focus in this paper is on the ecosystem rather than the behavior of any individual aggregate, the names are not being

¹Department of Physics, University of Miami, Coral Gables, FL 33126, USA. ²Department of International Studies, University of Miami, Coral Gables, FL 33126, USA.

³Department of Government, Harvard University, Cambridge, MA 02138, USA. ⁴Department of Geography and Regional Studies, University of Miami, Coral Gables, FL 33126, USA.

⁵Department of Computer Science, University of Miami, Coral Gables, FL 33126, USA. ⁶Center for Computational Science, University of Miami, Coral Gables, FL 33126, USA.

*Corresponding author. Email: wuchty@cs.miami.edu

released. They are available on request from the authors. Pro-ISIS aggregates inhabit an online environment in which predatory entities such as police cybergroups, individual hackers, and website moderators seek to shut down pro-ISIS activity and narratives (17, 18). In contrast to the largely mundane chatter that may casually mention ISIS on Twitter and in aggregates focused on sport, for example, pro-ISIS aggregates frequently discuss operational details such as routes for financing, technological know-how, and avoiding drone strikes. We chose VKontakte for our pro-ISIS analysis because (i) pro-ISIS aggregates are shut down essentially immediately on Facebook, but not on VKontakte; (ii) it is the largest European online social networking service, with more than 350 million users; (iii) it allows multiple languages and is used worldwide; (iv) being based in Russia, it has a high concentration of users of Chechen origin focused in the Caucasus region near ISIS’s main area of influence in the Levant; and (v) ISIS used it to spread propaganda among the Russian-speaking population (2).

Our methodology for identifying these pro-ISIS aggregates was as follows. We manually identified relevant narratives using hashtags in multiple languages—e.g., #isn, #khalafah, #fisyria, #игиш (i.e., ISIS), #дауля (i.e., *dawla*, meaning “state”), and #халифат (i.e., “Caliphate”)—and traced these to underlying aggregates. The specific criterion for inclusion in the list was that the group explicitly expressed its support for ISIS, publishing ISIS-related news or propaganda and/or calling for jihad in the name of ISIS. This list was fed into

software application programming interfaces that expanded it by means of automated search snowballing (fig. S2). The expanded aggregate list was then cross-checked to eliminate false identifications. New embedded links were manually searched to identify more aggregates and hashtags. We then iterated this process until closure of the aggregate list (i.e., the search led back to aggregates that were already in the list). Although this process was labor intensive, we were able to find closure on a daily basis in real time. A similar process was followed for the civil protest data.

We uncovered 196 pro-ISIS aggregates involving 108,086 individual followers between 1 January and 31 August 2015. On any given day, the total number of follows in the follower-aggregate network [i.e., the total number of links that existed on that day from followers (blue nodes) into the various aggregates (red nodes), as shown in the inset to Fig. 1) ranged up to 134,857. The data provided us with bipartite graphs in which individual members belong to aggregates but aggregates are not linked to each other except through people. This two-mode network has a highly complex temporal evolution—with strong heterogeneity in both the number of follows per individual follower (i.e., the number of links emanating from a given blue node) and the number of follows per aggregate (i.e., the number of links entering a given red node, which we define as the aggregate’s size)—and no obvious hierarchical structure. This suggests that the follower-aggregate dynamics are driven by self-organization. Such online support is likely a necessary but not sufficient condition for

any real-world actions to take place subsequently, because many additional factors can hinder real-world execution. However, Fig. 2 suggests that the online proliferation of pro-ISIS or protest aggregates can indeed act as an indicator of conditions becoming right for the onset of a real-world attack campaign or mass protests, respectively. We fit the trend in the creation dates of new online aggregates (Fig. 2, A and B) to a well-known organizational development curve (19). The escalation parameter b diverges at these real-world onsets (Fig. 2, C and D) and follows the same mathematical dependence $(T_c - t)^{-1}$ as a wide class of physical phase transitions (20), with the divergence date T_c matching the actual onset almost exactly (SM). The connection to physical phase transitions again suggests that self-organization is a driving factor (20). Although such a divergence will not necessarily preempt attacks involving only a few individuals, such as in San Bernardino or Paris, it can help indicate an alignment of favorable conditions and has the advantage that it does not rely on any real-world events having yet occurred or likely dates having been circulated through social media in advance (14–16). The far longer lifetimes for online aggregates of protestors in Fig. 2B, as compared with pro-ISIS aggregates in Fig. 2A, makes sense because predatory online shutdown pressure was far less for the civil protestors; in particular, we found no evidence of any shutdowns in Fig. 2B, in stark contrast to Fig. 2A. Figure 2D is likely smoother than Fig. 2C for the same reason. More aggressive antigovernment protests, such as the sudden outburst in Venezuela in February 2014 (fig. S6),

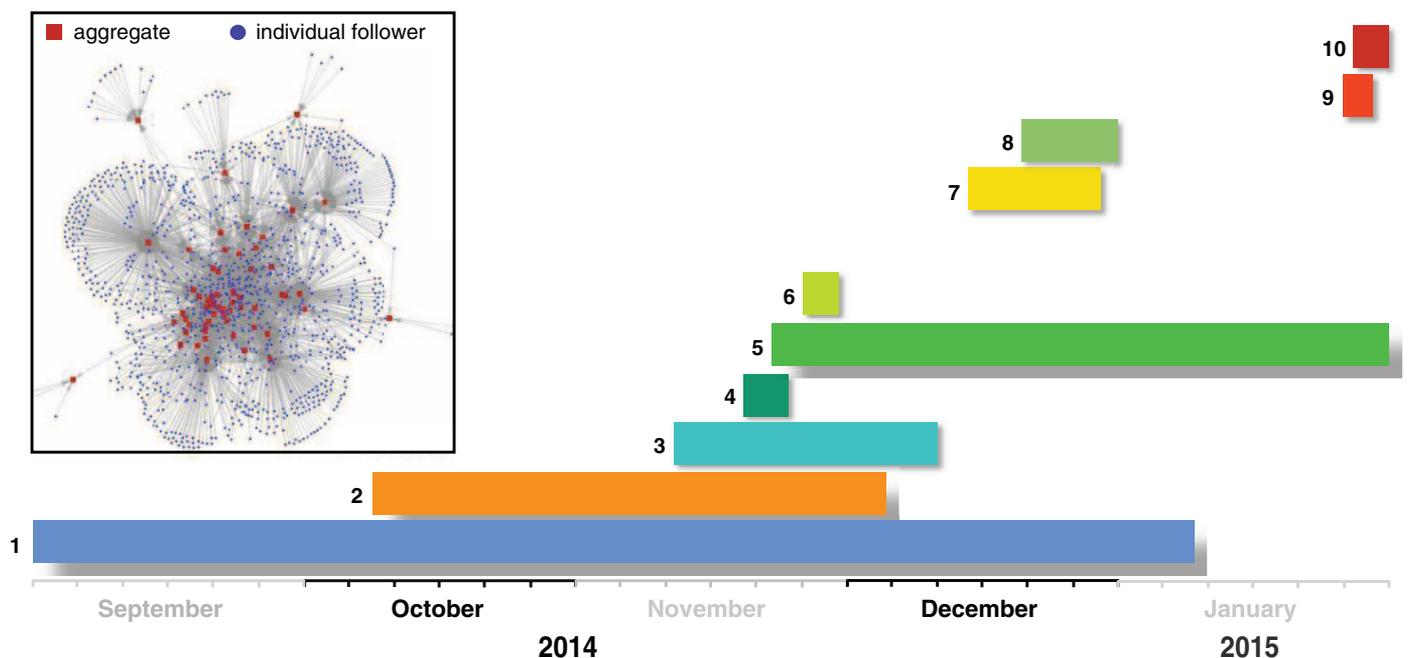


Fig. 1. Pro-ISIS aggregates. Horizontal bars illustrate timelines of some typical pro-ISIS aggregates. Their names are available from the authors. Each timeline starts when the aggregate appears and ends when it disappears. (Inset) Snapshot of part of an aggregate-follower network on 1 January 2015 showing individual followers (blue nodes) linking to pro-ISIS aggregates (red nodes). Followers can link into as many aggregates as they wish. Aggregates emerge of all sizes, where an aggregate’s size is the number of follows linking into it.

generate an intermediate case between Fig. 2, A and B.

We now develop a systems-level theory of this online aggregate ecology. The aggregate size variations observed empirically were characterized by distinctive shark-fin shapes (Fig. 3A), with each shutdown of a pro-ISIS aggregate severing the links into that particular aggregate—hence the abrupt drop. This fragmentation coexists with self-organized coalescence by which individual followers sporadically link into existing aggregates while existing aggregates sporadically link into each other. Although each aggregate's precise shark-fin shape will depend on its content and noticeability to external predators, Fig. 3 shows that the system-level features are captured using only this minimal coalescence-fragmentation process. At each time step, a phenomenological probability v_{coal} describes the sporadic addition of 1,2,3,... etc. follows to an aggregate (coalescence of followers), whereas v_{frag} describes the sporadic sudden shutdown of an aggregate (fragmentation of followers). Such stochastic shutdown is realistic because the predators (e.g., government monitors or individual hackers) are largely independent entities and can only shut down aggregates that they happen to find. Larger aggregates should be more noticeable; hence, we can take the prob-

ability of a particular aggregate being picked for coalescence or targeted for shutdown as proportional to the aggregate's size ($2I$), although this is generalizable to other algebraic forms without affecting our main findings (SM). The total number of potential followers N in the system is a sum, over all potential followers, of the maximum number of aggregates that each follower is prepared to follow. The number of follows per individual can be heterogeneous, and at any time step, not all N follows are necessarily used. Computer simulations of this coalescence-fragmentation process reproduce the ecology of shark-fin shapes of all sizes (Fig. 3B) with a power-law distribution $s^{-\alpha}$ for the time-average number of aggregates of size s where $\alpha = 2.5$. This is similar to the empirical value of $\alpha = 2.33$ that had high goodness-of-fit ($P = 0.86$) (Fig. 3C). These shark-fin dynamics are robust in that they emerge irrespective of when we examine the model's evolution (Fig. 3B) and for any value of N as a result of the model's self-similarity—i.e., the coalescence-fragmentation process generates the same dynamics across all aggregate sizes (22). Connecting to real-world ISIS activity, we note that the severity of ISIS attacks is also approximately power-law distributed with exponent $\alpha = 2.44$ and goodness-of-fit $P > 0.1$. The model can be represented mathematically by the

following coupled, nonlinear differential equations describing the number n_s of pro-ISIS aggregates of size s ($s > 1$) over time.

$$\frac{\partial n_s(t)}{\partial t} = \frac{v_{\text{coal}}}{N^2} \sum_{k=1}^{s-1} k(s-k)n_k(t)n_{s-k}(t) - \frac{2v_{\text{coal}}s n_s(t)}{N^2} \sum_{k=1}^{\infty} k n_k(t) - \frac{v_{\text{frag}} s n_s(t)}{N} \quad (1)$$

A detailed discussion of Eq. 1 is given in the SM. Like the data and computer simulation, solving Eq. 1 mathematically yields a power-law $s^{-\alpha}$ for the time-averaged aggregate size, with an exact exponent $\alpha = 2.5$ [see (23, 24) and SM for the mathematical proof]. The spatial independence of Eq. 1 is consistent with online interactions being largely independent of followers' separation across the globe. The first term on the right describes the formation of an aggregate of size s (i.e., s follows) from a smaller one through the addition of 1,2,3,... etc. new follows; the second describes the loss of an aggregate that coalesced with another aggregate; and the third describes the fragmentation of an aggregate of size s . $n_{s-1}(t)$ is the pool of isolated (i.e., unused) follows at time t —i.e., potential “recruits”, with $\sum_{s=1}^{\infty} n_s(t) = N$. We take

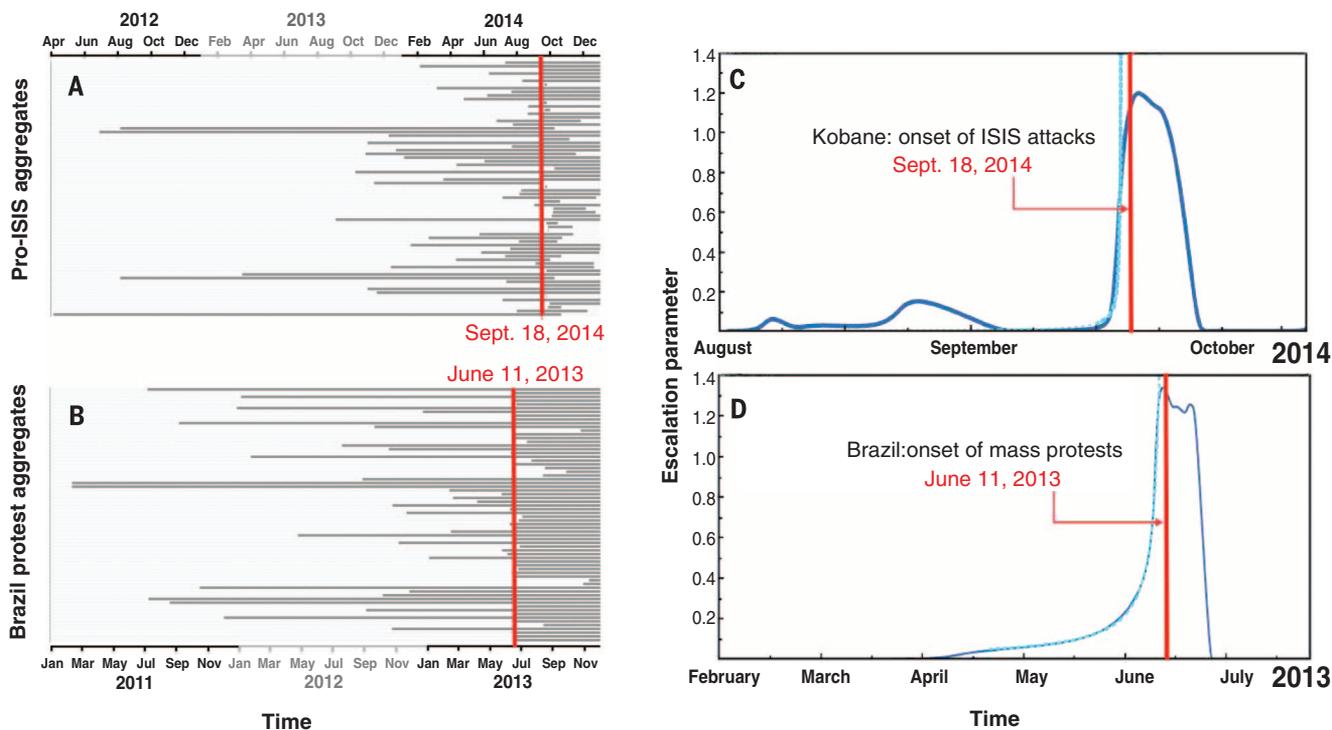


Fig. 2. Proliferation in online aggregate creation before the onsets of recent real-world campaigns (red vertical lines). (A and C) concern the unexpected assault by ISIS on Kobane in September 2014. (B and D) concern the unexpected outburst of protests in Brazil in June 2013, commonly termed the “Brazil Winter,” which involved some violence and for which we were able to collect accurate information following the Intelligence Advanced Research Projects Activity (IARPA) OSI program (14, 15). Horizontal bars in (A) and (B) show timelines for (A) pro-ISIS aggregates on VKontakte and (B) protestor

aggregates on Facebook in Brazil. Each horizontal bar represents one aggregate. The aggregates are stacked separately along the vertical axis. [(C) and (D)] Divergence of escalation parameter b for aggregate creation (dark blue solid line) coincides with real-world onset at time T_c (vertical red line). The light blue dashed line shows theoretical onset $(T_c - t)^{-1}$. The subsequent decrease in both curves likely occurs for system-specific reasons associated with coalition bombings starting in (C) and loss of public interest in (D).

N to be reasonably slowly varying, although this can be generalized (SM). Adding heterogeneity to the aggregate formation process (e.g., preference for similar or diverse follows) leaves the exponent $\alpha = 2.5$ unchanged, as do a variety of other generalizations (table S2) (23, 24).

Our theoretical model generates various mathematically rigorous yet operationally relevant predictions. First, anti-ISIS agencies can thwart development of large aggregates that are potentially far more potent (27) by breaking up smaller ones. As shown in Fig. 3D, adding a simple cost into the model for shutting down an aggregate makes this strategy actually more effective than targeting the largest aggregates (SM). Second, if anti-ISIS agencies are insufficiently active in countermeasures and hence the overall rate at which they fragment pro-ISIS clusters becomes too small—specifically, if the aggregate fragmentation rate $v_{\text{frag}} < (N \ln N)^{-1}$ —then pro-ISIS support will grow exponentially fast into one super-aggregate (fig. S11). Third, when fragmentation rates drop below a critical value $v_{\text{frag}}^{\text{critical}}$, the system enters a regime in which any piece of pro-ISIS material can spread globally across the pro-ISIS support network through contagion: $v_{\text{frag}}^{\text{critical}} = v_{\text{coal}} p/q$, with p and q representing the probabilities of follower-to-follower transmission and follower recovery, respectively (25). To prevent diffusion of potentially dangerous material and ideas, the fragmen-

tation rate should be greater than $v_{\text{coal}} p/q$. Fourth, any online “lone wolf” actor will only truly be alone for short periods of time (on the order of weeks in Fig. 3A, for example) before being attracted into one aggregate or another through coalescence. Fifth, a systems-level tool emerges for detecting the future online emergence of new ISIS-like entities, which is to employ our methodology to determine whether a crude power-law distribution with α near 2.5 begins to emerge for aggregate support surrounding a particular theme.

At a more microscopic level, the data reveal that pro-ISIS aggregates exhibit the ability to collectively adapt in a way that can extend their lifetime and increase their maximal size (Fig. 4), despite the fact that each aggregate is an ad hoc group of followers who likely have never met, do not know each other, and do not live in the same city or country. For the civil protests, by contrast, we detected no such adaptations and no online predatory shutdowns, adding support to the notion that the pro-ISIS adaptations are a response to their high-pressured online environment. Figure 4, A to C, illustrates the remarkable speed, variety, and novelty of these adaptations, with 15% of aggregates exhibiting name changes; 7% exhibiting flips between online visibility (i.e., content open to any VKontakte user) and invisibility (i.e., content open only to current followers of the aggregate); and 4% exhibiting reincarnation in which

an aggregate disappears completely and then re-emerges at a later time with another identity but with most (e.g., >60%) of the same followers. Such reincarnation is not known to occur in real-world ecologies of living organisms. Figure 4D confirms that these adaptations tend to increase not only the maximum number of followers attracted into the aggregate (maximum size) but also its lifetime. The 0.9 value for the reincarnation lifetime can be understood as follows: Reincarnation involves the aggregate temporarily disappearing; therefore, an aggregate that uses reincarnation runs a high risk of losing followers because they do not know when, and with what identity, the core follower group will reemerge. Reincarnation hence tends to be used by aggregates that are attracting unusually high predation and would otherwise have had a much shorter lifetime. Reincarnation extends this lifetime beyond its otherwise much shorter value, but not enough to reach the value of 1 corresponding to aggregates that experience less intense shutdown pressure and hence do not employ adaptations. These observations open up the possibility to add evolutionary game theoretic features into our systems-level theory to explain the multiple use of particular adaptations by particular aggregates and their decision of when to adapt. A future generalized theory could prove possible, employing game theoretic ideas from (26), for example.

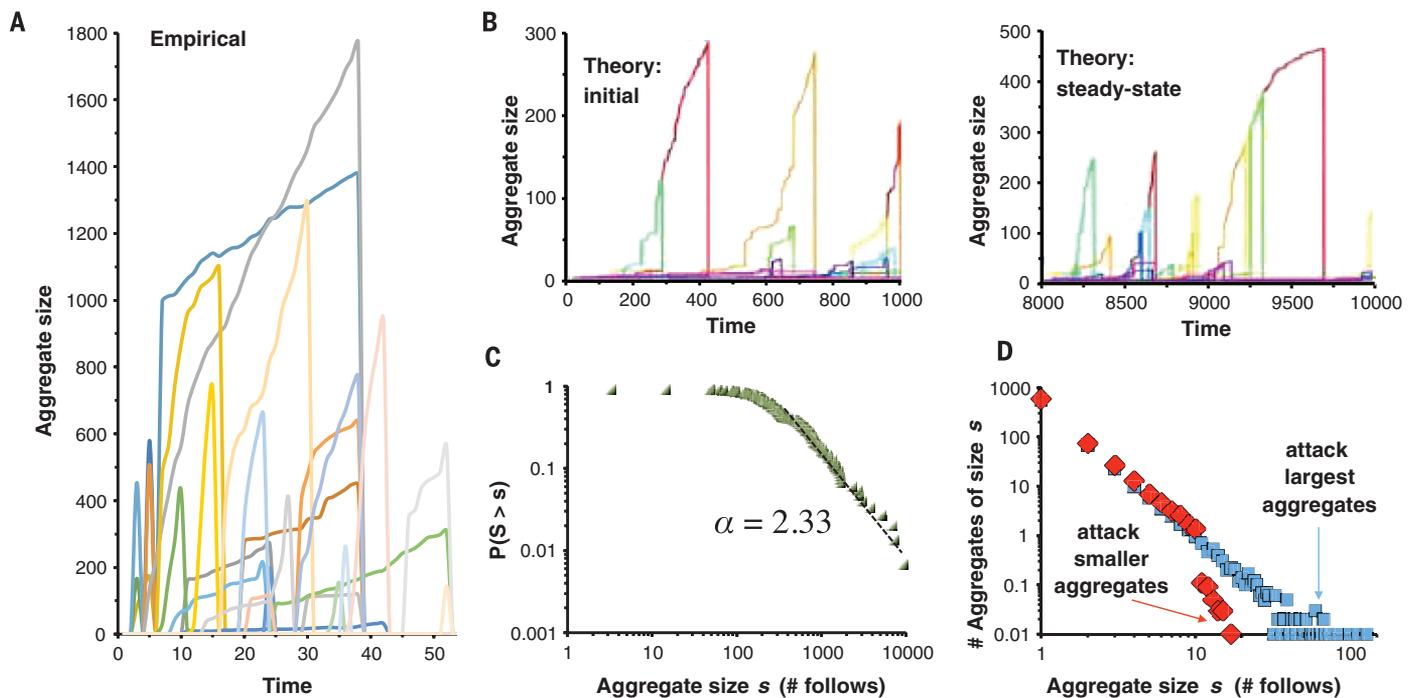


Fig. 3. Size dynamics of pro-ISIS aggregates. (A) Empirical size variation of pro-ISIS aggregates. Shark-fin shapes of all sizes emerge with shutdowns that are not strongly correlated. (B) Similar results are predicted by our theoretical model, irrespective of whether we consider the model’s initial (left) or steady-state (right) dynamics. Here, the total number of potential followers is $N = 500$; however, the model’s self-similar dynamics generate the same picture for any N with shark-fin shapes of all sizes. An aggregate grows by an individual linking in (i.e., size increases by 1) or by an existing aggregate linking in (i.e., size

increases by >1), as shown by the color change. In (B), knowledge of the theory’s microscopic dynamics allows us to denote each coalescence of a large aggregate by a color change, whereas in the empirical data (A), we maintain a constant color for each aggregate. (C) Complementary distribution function for the observed aggregate sizes. (D) Effect of intervention strategy involving dismantling smaller aggregates (SM). Using a larger N increases the vertical and horizontal scales without changing the main results (see fig. S10). Red diamonds: $s_{\text{min}} = 10$ and $s_{\text{max}} = 50$. Blue squares: $s_{\text{min}} = 200$ and $s_{\text{max}} = 1000$.

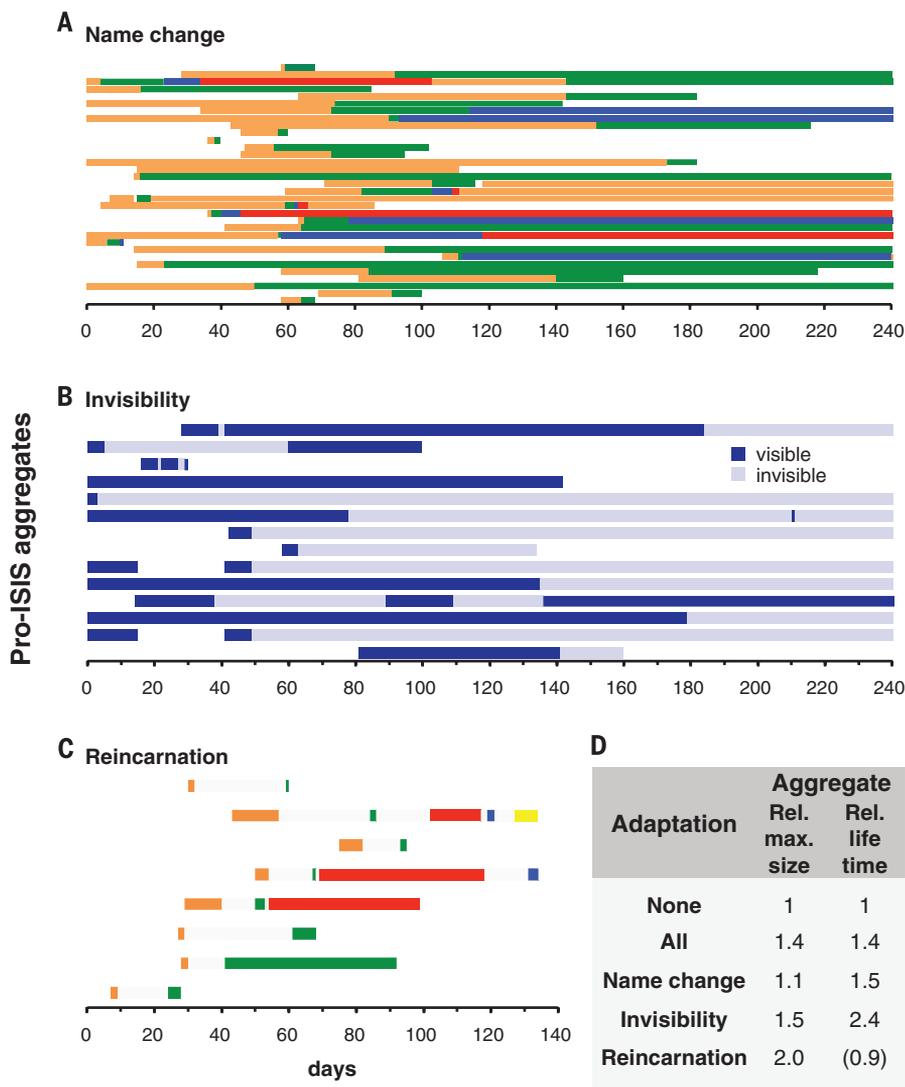


Fig. 4. Evolutionary adaptations. (A to C) Sample of pro-ISIS aggregate timelines showing evolutionary adaptations (shown by switches in colors) that tend to increase an aggregate's maximum attained size and extend its lifetime (D). Time is measured in days from 1 January 2015. In (A), the switch in colors within a given timeline indicates a switch in aggregate name. (B) Dark blue means the aggregate is visible (i.e., content open to any VKontakte user), while light blue means it is invisible (i.e., content open only to current followers of the aggregate). (C) Aggregate has a specific initial identity (orange), then disappears from the Internet for an extended time (white), then reappears with another identity shown by a switch in color. (D) Relative maximum aggregate size and relative lifetime for particular adaptations and their combinations, given as average values relative to the values for aggregates employing no adaptation. "All" corresponds to aggregates that use name change, invisibility, and reincarnation. See the text for explanation of the "(0.9)" entry.

More generally, our findings suggest that instead of having to analyze the online activities of many millions of individual potential actors worldwide (27), interested parties can shift their focus to aggregates, of which there will typically be only a few hundred. Our approach, combining automated data-mining with subject-matter expert analysis and generative model-building drawn from the physical and mathematical sciences, goes beyond existing approaches to mining such online data (28–30). Although recent reports (31) suggest that the amount of explicit pro-ISIS material

online may have declined since summer 2015, it is possible that there is lower detection due to novel adaptations being employed—as in Fig. 4, but now likely more sophisticated.

REFERENCES AND NOTES

- M. Weiss, H. Hassan, *ISIS: Inside the Army of Terror* (Regan Arts, New York, 2015).
- BBC News, "Russian students targeted as recruits by Islamic State"; <http://linkis.com/dmFgu> (24 July 2015).
- P. Gill, J. Lee, K. Rethemeyer, J. Horgan, V. Asal, *Int. Interact.: Empir. Theor. Res. Int. Relat.* **40**, 52–78 (2014).
- R. Wrangham, L. Glowacki, *Hum. Nat.* **23**, 5–29 (2012).

- J. E. Smith *et al.*, *Trends Ecol. Evol.* **31**, 54–66 (2016).
- M. Kenney *et al.*, *Appl. Ergon.* **44**, 739–747 (2013).
- J. N. Shapiro, *The Terrorist's Dilemma: Managing Violent Covert Organizations* (Princeton Univ. Press, 2013).
- A. M. Morgenstern *et al.*, *Am. J. Phys.* **81**, 805 (2013).
- G. King, J. Pan, M. E. Roberts, *Science* **345**, 1251722 (2014).
- D. J. Watts, P. S. Dodds, *J. Consum. Res.* **34**, 441–458 (2007).
- F. Karimi, C. E. Shoichet, D. Ford, "San Bernardino shooters were radicalized 'for quite some time,' FBI says." CNN News, 7 December 2015; www.cnn.com/2015/12/07/us/san-bernardino-shooting/index.html.
- V. S. Subrahmanian, A. Mannes, A. Silva, J. Shakaran, J. P. Dickerson, *Computational Analysis of Terrorist Groups: Lashkar-e-Taiba* (Springer, New York, 2013).
- P. Gill, *Lone Actor Terrorists: A Behavioural Analysis* (Routledge, London, 2015).
- P. Manrique *et al.*, Context matters: Improving the uses of big data for forecasting civil unrest: Emerging phenomena and big data. *IEEE Intelligence and Security Informatics* (IEEE, 2013), pp. 169–172.
- J. Matheny, Test and evaluation in ACE and OSI IARPA (2013); available online at http://semanticcommunity.info/@api/deki/files/21696/3-ACE_and_OSI_NIST_Brief.pdf.
- J. Cadena *et al.*, *PLOS ONE* **10**, e0128879 (2015).
- BBC News, "Anonymous targets IS sympathisers on Twitter"; www.bbc.com/news/technology-33608369 (21 July 2015).
- BBC News, "Islamic State web accounts to be blocked by new police team"; www.bbc.com/news/world-europe-33220037 (22 June 2015).
- N. Johnson *et al.*, *Science* **333**, 81–84 (2011).
- A.-L. Barabasi, H. E. Stanley, *Fractal Concepts in Surface Growth* (Cambridge University Press, 1995).
- V. Asal, S. M. Chermak, S. Fitzgerald, J. D. Freilich, *Crim. Justice Rev.* **2016**, 10.1177/0734016815626970 (2016).
- N. F. Johnson, P. Jefferies, P. M. Hui, *Financial Market Complexity* (Oxford Univ. Press, 2003), chap. 5.
- J. C. Bohorquez, S. Gourley, A. R. Dixon, M. Spagat, N. F. Johnson, *Nature* **462**, 911–914 (2009).
- B. Rusczycki, B. Burnett, Z. Zhao, N. F. Johnson, *Eur. Phys. J.* **72**, 289–302 (2009).
- Z. Zhao *et al.*, *Phys. Rev. E Stat. Nonlin. Soft Matter Phys.* **81**, 056107 (2010).
- M. A. Nowak, *Evolutionary Dynamics: Exploring the Equations of Life* (Belknap Press, New York, 2006).
- N. Perra *et al.*, *Phys. Rev. Lett.* **109**, 238701 (2012).
- D. Koutra, D. Jin, Y. Ning, C. Faloutsos, Perseus: An interactive large-scale graph mining and visualization tool (DEMO), VLDB 2015, Kohala Coast, Hawaii, 31 August to 4 September 2015.
- Q. Zhao, M. Erdogdu, H. He, A. Rajaraman, J. Leskovec, SEISMIC: A self-exciting point process model for predicting tweet popularity, ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), Sydney, 10 to 13 August 2015.
- A. Stanton, A. Thart, A. Jain, P. Vyas, A. Chatterjee, P. Shakarian, arXiv:1508.01192v1 (2015).
- J. M. Berger, H. Perez, The Islamic State's diminishing returns on Twitter. GW Program on Extremism (2016); available at https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Berger_Occasional%20Paper.pdf.

ACKNOWLEDGMENTS

N.F.J. gratefully acknowledges partial support for preliminary work from Intelligence Advanced Research Projects Activity (IARPA) under grant D12PC00285 and recent funding under National Science Foundation (NSF) grant CNS1500250 and Air Force (AFOSR) grant 16RT0367. The views and conclusions contained herein are solely those of the authors and do not represent official policies or endorsements by any of the entities named in this paper. Data described are presented in an Excel file available in the supplementary materials, and code is provided in the SM document.

SUPPLEMENTARY MATERIALS

www.sciencemag.org/content/352/6292/1459/suppl/DC1
Materials and Methods
Supplementary Text
Figs. S1 to S12
Tables S1 to S3
Database S1
References

13 December 2015; accepted 12 May 2016
10.1126/science.aaf0675



New online ecology of adversarial aggregates: ISIS and beyond

N. F. Johnson, M. Zheng, Y. Vorobyeva, A. Gabriel, H. Qi, N. Velasquez, P. Manrique, D. Johnson, E. Restrepo, C. Song and S. Wuchty (June 16, 2016)
Science **352** (6292), 1459-1463. [doi: 10.1126/science.aaf0675]

Editor's Summary

Tackling the advance of online threats

Online support for adversarial groups such as Islamic State (ISIS) can turn local into global threats and attract new recruits and funding. Johnson *et al.* analyzed data collected on ISIS-related websites involving 108,086 individual followers between 1 January 1 and 31 August 2015. They developed a statistical model aimed at identifying behavioral patterns among online supporters of ISIS and used this information to predict the onset of major violent events. Sudden escalation in the number of ISIS-supporting ad hoc web groups ("aggregates") preceded the onset of violence in a way that would not have been detected by looking at social media references to ISIS alone. The model suggests how the development and evolution of such aggregates can be blocked.

Science, this issue p. 1459

This copy is for your personal, non-commercial use only.

Article Tools Visit the online version of this article to access the personalization and article tools:
<http://science.sciencemag.org/content/352/6292/1459>

Permissions Obtain information about reproducing this article:
<http://www.sciencemag.org/about/permissions.dtl>

Science (print ISSN 0036-8075; online ISSN 1095-9203) is published weekly, except the last week in December, by the American Association for the Advancement of Science, 1200 New York Avenue NW, Washington, DC 20005. Copyright 2016 by the American Association for the Advancement of Science; all rights reserved. The title *Science* is a registered trademark of AAAS.