

Genau das Wichtige wissen:

Terrorgefahr DNS-Synthese?

Von **Emily Singer**



Quelle: Openwetware.org

*Im Bereich der synthetischen Biologie tut sich derzeit viel. Forscher entwickeln ganz neue Organismen, die unser aller Leben verbessern sollen - Bakterien, die Energie produzieren können, Viren, die Medikamentenwirkstoffe abgeben und andere neuartige, künstliche biologische Einheiten (mehr dazu im TR-Artikel "**Biomachinesbau**"[1]). Doch bei aller Euphorie hat der Sektor auch eine dunkle Seite.*

Diese betrifft vor allem die so genannte DNS-Synthese, bei denen Forscher DNS-Teile von Spezialfirmen auf der ganzen Welt bestellen und dann beliebig neu zusammensetzen, um biologische "Ersatzteile" zu schaffen. Mit der gleichen Technologie können aber nicht nur wertvolle Innovationen, sondern auch Biowaffen entstehen. Die (zunächst einmal hypothetische) Horrorgeschichte: Terroristen könnten sich DNS bei einem Synthese-Anbieter bestellen, um dann den Pocken-Erreger oder eine noch tödlichere Krankheit nachzubauen. Zwar glauben die meisten

Experten bislang nicht, dass Terrorkommandos bereits über das Knowhow verfügen, derart komplexe biochemische Arbeiten durchzuführen. Dennoch warnen Wissenschaftler, dass die Technologie immer kostengünstiger und leichter zu handhaben wird. Und genau damit wachse das Gefahrenpotenzial.

*Auf der "**Synthetic Biology 2.0**"-Konferenz[2] (SB2), die kürzlich im kalifornischen Berkeley stattfand, widmeten die Forscher einen ganzen Tag dem Thema **Sicherheit**[3] in diesem aufstrebenden Wissenschaftsgebiet. Das Ergebnis war der **Entwurf für eine offizielle Deklaration**[4], die Richtlinien vorschlägt, mit denen Forscher wie Firmen ihre Arbeit künftig durchführen sollen.*

*So will die Wissenschaft etwa eine verbesserte Software entwickeln, die erkennen soll, wenn gefährliche DNS-Sequenzen bei DNS-Synthese-Firmen bestellt werden. Und: Forscher sollen künftig nur noch mit Unternehmen arbeiten, die solche Sicherheitswerkzeuge auch einsetzen. **Drew Endy**[5], Bioingenieur am MIT, gehörte als Organisator der SB2 zum Team, das an dem Richtlinien-Entwurf arbeitete. Im Interview mit Technology Review spricht er über die Sicherheitsdiskussion auf der Konferenz und darüber, was die Deklaration im Bereich der DNS-Synthese erreichen soll.*

Technology Review: Herr Endy, welche Bereiche in Ihrem Forschungsfeld machen Ihnen die meisten Sorgen?

Drew Endy: Mit dem Fortschritt, den die synthetische Biologie in den letzten paar Jahren durchmachte, ergaben sich für uns nahezu sofort mehrere Problemkomplexe, die mit der Schnittstelle zwischen Technologie und Gesellschaft zu tun haben. Kurzgefasst kann man hier vier Themenbereiche nennen: Sicherheit, Patente und Weitergabe der Technik, öffentliche Wahrnehmung und Verständnis für die Technik sowie die interne Organisation unserer Wissenschafts-Community. Es ist unverantwortlich, eine neue Technologie zu entwickeln, ohne die damit verbundenen direkten nichttechnischen Probleme anzusprechen.

Heutzutage überprüfen beispielsweise einige DNS-Synthese-Firmen gar nicht, was sie da herstellen. Der britische "Guardian" demonstrierte dies kürzlich in einem Artikel auf der Titelseite, in dem beschrieben wurde, dass man Pocken-DNS per Mailorder bestellen könne. Wir haben dann versucht, den Journalisten davon abzubringen, dieses Experiment tatsächlich durchzuführen.

TR: Auf der SB2 hat die Wissenschaftsgemeinschaft nun eine explizite Deklaration erarbeitet, die Ziele und Regelungen enthält, die beginnen, die Sicherheitsprobleme der DNS-Synthese zu adressieren. Was sind hier die Hauptpunkte?

Endy: Als erstes wollen wir sicherstellen, dass in der DNS-Synthese-Technik die gleichen Überwachungsinstitutionen und Forschergremien entstehen, wie sie bereits in den vergangenen 30 Jahren in der regulären Gentechnik Praxis sind. Das Hauptproblem dabei ist, dass man inzwischen dank Internet zunehmend anonym auf die DNS-Synthese zugreifen kann. Deshalb bitten wir alle Unternehmen auf diesem Gebiet, ein offenes Sicherheitsgrundkonzept zu schaffen, das sicherstellt, dass alle Bestellungen bei diesen Firmen nur von qualifizierten Personen kommen können, die zur Handhabung der bestellten DNS auch befugt sind.

Ein solches Grundkonzept ist aber nur dann effizient, wenn es überall verwendet wird. Deshalb legen wir den Wissenschaftlern nahe, Druck auf die DNS-Synthese-Firmen auszuüben, sich diesen Standards anzuschließen. Der Rest der Deklaration enthält die Forderung, einen offenen und konstruktiven Dialog anzustoßen, der die verbleibenden Themen anspricht - etwa den Bereich der Patente und der Weitergabe der Technik.

TR: Sind Sie für einen Boykott aller Firmen, die nicht vorher prüfen, welche Form von DNS sie da synthetisieren?

Endy: Derzeit noch nicht. Die Technologie, um diese Bestellungen auch überprüfen zu können, ist noch lange nicht perfekt und wäre in manchen Bereichen auch unpraktisch - etwa bei der Massenproduktion sehr kleiner DNS-Fragmente. Unser erstes Ziel ist es, Firmen, die sich ansonsten Konkurrenz machen, nun zu einer Zusammenarbeit zu bewegen und ihre Sicherheitstechnik mit der Regierung und anderen Gruppierungen zu koordinieren, um bestehende Probleme zu lösen. Mit verbesserten Prüfmethoden, die weitläufig eingesetzt werden, hoffen wir dann, dass sich das beste Verfahren durchsetzt. Wenn es hier jedoch keinen Fortschritt gibt, braucht's durchaus deutlichere Worte - und Taten.

TR: Ein anderes Ergebnis der Diskussionen auf der SB2 ist die Gründung einer Industrieorganisation, der sich DNS-Synthese-Firmen anschließen können. Welches Ziel hat sie?

Endy: Jeder, der eine DNS-Synthese-Firma leitet, hat das gleiche Problem - er oder sie muss prüfen, was da hergestellt wird, damit nicht unfreiwillig Material entsteht, das schädlich sein könnte - für Firmenangehörige, Lieferpersonal oder andere Personen. Mit der Industrieorganisation lässt sich hier eine gemeinsame Lösung finden, in die man dann gemeinsam investieren kann. So entsteht eine bessere Technologie, als wenn man das Problem allein angehen würde. Eine effiziente Zusammenarbeit und eine starke Führung sind hier gefragt.

TR: Welche Rolle haben Sie selbst in dieser neuen Organisation?

Endy: Wir sind derzeit dabei, die Gruppe voranzutreiben, in dem wir uns um politische Unterstützung bemühen. Ich halte es für unverantwortlich, wenn die akademische Forschungswelt nur nach einer Lösung schreien würde, ohne an ihr mitzuarbeiten. Die Organisation selbst wird aber universitätsunabhängig sein.

TR: Auf der SB2 gab es das Statement eines Abgesandten einer DNS-Synthese-Firma, in dem darüber geklagt wurde, wie schwer es sei, die Regierung dazu zu bewegen, bei der Überprüfung von Bestellungen mitzuarbeiten. Er beschrieb, wie er eine Bestellung mit einer potenziell gefährlichen Sequenz erhalten hatte. Er rief dann bei verschiedenen Regierungsstellen an, um herauszufinden, was er nun tun könne. Niemand konnte ihm helfen.

Endy: Dieses Problem kennen wir in den USA bereits seit sechs Jahren. Wir können einfach keine Kontaktperson innerhalb der Regierung finden, die uns helfen kann. Auch aus diesem sehr offensichtlichen Grund wird es Zeit, eine Industrieorganisation zu bilden, die dann als Anlaufpunkt dienen kann, über den dann die Regierung und die entsprechenden Aufsichtsbehörden kontaktiert werden kann.

TR: Eine der Hauptaufgaben der neuen Organisation wird sein, die Entwicklung einer neuen Prüfsoftware voranzutreiben. Wie funktionieren die aktuell verfügbaren Lösungen?

Endy: Ein Beispiel wäre ein Stück Code namens "BlackWatch", das von Rob Jones bei Craic Computing entwickelt wurde. Das Programm prüft, ob man nicht gerade unwissentlich dabei ist, eine DNS-Sequenz zu erzeugen, die auf einer schwarzen Liste mit Erregern steht.

TR: Welche Probleme macht diese Software noch?

Endy: Sie produziert unter anderem eine hohe Zahl von Fehltreffern. Vergleicht man die angeforderte Sequenz mit der Anzahl an Sequenzen, die das gesamte Genom eines gefährlichen Bakteriums umfassen, sehen viele dieser Gene so aus wie das in der Forschung viel verwendete E. coli. Es dauert sehr lange, bis man herausgefunden hat, was wirklich gefährlich ist und was nicht - und es ist entsprechend teuer. Nicht selten wird ein Wissenschaftler herangezogen, der dann die Entscheidung von Hand trifft.

Ein zweites Problem: Es wäre naiv zu glauben, ein Computerprogramm könne sich DNS-Sequenzen ansehen, um dann zu erkennen, was der Käufer da eigentlich zusammenbauen will. Software muss Teil eines Entscheidungsprozesses sein, der mehrere Fragestellungen enthält: Wer bestellt die DNS und wohin wird sie verschickt? Genauso wichtig ist es, dass die Personen, die das Material bestellen, und das Land, in dem es dann landet, Grundregeln der Biosicherheit einhalten.

TR: Wie könnte eine neue Software denn dann aussehen?

Endy: Wir müssen dabei vorab ein paar grundlegende Fragen klären. Was macht eine DNS-Sequenz gefährlich? Lässt sich etwas Natürliches im Vergleich zu etwas Künstlichem unterscheiden? Das ist ein ganz neuer Forschungsprozess mit zahlreichen Vorschlägen für die Herangehensweise.

TR: Einige Beobachter meinen, die größte Gefahr gehe von geheimen Regierungsprogrammen aus, weil Regierungen die Parteien seien, die die Ressourcen besitzen, mit DNS-Material überhaupt derart zu arbeiten. Kann Ihre Deklaration auch dagegen helfen?

Endy: Nein, das Problem, dass eine Regierung ein geheimes Biowaffenprogramm starten könnte, wird nicht adressiert. Indirekt kann eine technisch überlegene, offene Forschungsgemeinschaft aber dabei helfen, diese potenzielle Gefahr zu verkleinern. Ohne eine solche dürfte sie sicher zunehmen.

Übersetzung: Ben Schwan.

Mehr zur Synthetischen Biologie finden Sie im TR-Artikel "**Biomachinesbau**"[6].

(nbo-tr[7]/Technology Review)

URL dieses Artikels:

<http://www.heise.de/tr/artikel/75429>

Links in diesem Artikel:

- [1] <http://www.heise.de/tr/artikel/72848>
- [2] <http://pbd.lbl.gov/sbconf/>
- [3] <http://www.heise.de/tr/blog/artikel/73577>
- [4] <http://pbd.lbl.gov/sbconf/SB.v5%5B1%5D.pdf>
- [5] <http://web.mit.edu/be/people/andy.htm>
- [6] <http://www.heise.de/tr/artikel/72848>
- [7] <mailto:nbo-tr@tr.heise.de>

Copyright © 2009 Heise Zeitschriften Verlag

International: [The H](#), [The H Security](#), [The H Open Source](#), [heise online Polska](#), [heise Security Polska](#), [heise Open Source Polska](#), [heise Networks Polska](#)

[Datenschutzhinweis](#)

[Impressum](#)

[Kontakt](#)